

VES-1616F-3x Series

VDSL Switch

User's Guide

Version 3.60

5/2007

Edition 2



About This User's Guide

Intended Audience

This manual is intended for people who want to configure the Switch series VDSL switch using the web configurator or via commands. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

Related Documentation

- Web Configurator Online Help
Embedded web help for descriptions of individual screens and supplementary information.
- Supporting Disk
Refer to the included CD for support documents.
- ZyXEL Web Site
Please refer to www.zyxel.com for additional support documentation and product certifications.

User Guide Feedback

Help us help you. Send all User Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,
ZyXEL Communications Corp.,
6 Innovation Road II,
Science-Based Industrial Park,
Hsinchu, 300, Taiwan.
E-mail: techwriters@zyxel.com.tw

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.



Warnings tell you about things that could harm you or your device.












Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The VES-1616F-34 or VES-1616F-35 may be referred to as the “Switch”, the “device”, the “system” or the “switch” in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the “enter” or “return” key on your keyboard.
- “Enter” means for you to type one or more characters and then press the [ENTER] key. “Select” or “choose” means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the “metric” value or the “scientific” value. For example, “k” for kilo may denote “1000” or “1024”, “M” for mega may denote “1000000” or “1048576” and so on.
- “e.g.” is a shorthand for “for instance”, and “i.e.” means “that is” or “in other words”.

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The Switch icon is not an exact representation of your device.

Switch 	Computer 	Server 
Notebook computer 	DSLAM 	Gateway 
Central Office/ ISP 	Internet 	Hub/Switch 

Safety Warnings



For your safety, be sure to read and follow all warning notices and instructions.

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe). For DC models, use DC power supply input of -48V DC to -60V DC, 1.5A Max no tolerance.
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the power outlet.
- The length of exposed(bared) power wire should not exceed 7mm.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Wire Gauge Specifications:Ground Wire: 18 AWG or larger for Ground Wire or Power Wire.
- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- Connect the POTS line and VDSL line test pin (TNV Circuit) according to CSA60950-1 2.1.3 Protection in restricted access locations section. 避免危險，此區域必需為專業人員方可進入及操作

This product is recyclable. Dispose of it properly.



Table of Contents

About This User's Guide	3
Document Conventions.....	4
Safety Warnings.....	6
Table of Contents.....	9
Contents Overview	19
List of Figures	21
List of Tables.....	25
Part I: Introduction.....	29
Chapter 1	
Getting to Know Your Switch.....	31
1.1 Introduction	31
1.2 Applications	31
1.2.1 MTU Application	31
1.2.2 Curbside Application	32
1.3 Ways to Manage the Switch	32
1.4 Good Habits for Managing the Switch	33
Chapter 2	
Hardware Installation.....	35
2.1 Mounting the Switch on a Rack	35
2.1.1 Rack-mounted Installation Requirements	35
2.1.2 Attaching the Mounting Brackets to the Switch	36
2.1.3 Mounting the Switch on a Rack	36
Chapter 3	
Hardware Overview.....	37
3.1 Front Panel Connection	37
3.1.1 VDSL and POTS Connections	37
3.1.2 Gigabit Ethernet Ports	38
3.1.3 Mini-GBIC Slots	38
3.1.4 Console Port	39

3.1.5 Power Connector	40
3.2 LEDs	40
 Part II: Status and Basic	43
 Chapter 4	
The Web Configurator	45
4.1 Introduction	45
4.2 System Login	45
4.3 The Status Screen	46
4.3.1 Change Your Password	50
4.4 Switch Lockout	50
4.5 Resetting the Switch	51
4.5.1 Reload the Configuration File	51
4.6 Logging Out of the Web Configurator	52
4.7 Help	52
 Chapter 5	
System Status and Port Statistics	53
5.1 Overview	53
5.2 Port Status Summary	53
5.2.1 VDSL Summary	54
5.2.2 VDSL Port Details	55
5.2.3 Ethernet Port Details	59
 Chapter 6	
Basic Setting	63
6.1 Overview	63
6.2 System Information	63
6.3 General Setup	65
6.4 Introduction to VLANs	67
6.5 Switch Setup Screen	68
6.6 IP Setup	69
6.6.1 Management IP Address	70
6.7 Port Setup	72
6.8 VDSL Parameters	75
6.8.1 Frequency Band Plan	75
6.8.2 Configured Versus Actual Rate	75
6.8.3 PSD	76
6.8.4 UPBO	76
6.8.5 Latency Modes	76

6.8.6 Rate Adaption	76
6.8.7 RFI (Radio Frequency Interference)	77
6.8.8 VDSL Profiles	77
6.9 VDSL Profile Setup	77
6.10 VDSL Alarm Profile Setup	80
6.11 VDSL PSD Profile Setup	82
 Part III: Advanced.....	 85
 Chapter 7	
VLAN	87
7.1 Introduction to IEEE 802.1Q Tagged VLAN	87
7.1.1 Forwarding Tagged and Untagged Frames	87
7.2 Automatic VLAN Registration	88
7.2.1 GARP	88
7.2.2 GVRP	88
7.3 Port VLAN Trunking	89
7.4 Select the VLAN Type	89
7.5 Static VLAN	89
7.5.1 Static VLAN Status	90
7.5.2 Configure a Static VLAN	91
7.5.3 Configure VLAN Port Setting	92
7.6 Port-based VLAN	93
7.6.1 Configure a Port-based VLAN	93
 Chapter 8	
Static MAC Forward Setup.....	97
8.1 Static MAC Forwarding Overview	97
8.2 Configuring Static MAC Forwarding	97
 Chapter 9	
Filtering.....	99
9.1 Filtering Overview	99
9.2 Configure a Filtering Rule	99
 Chapter 10	
Spanning Tree Protocol.....	101
10.1 STP/RSTP Overview	101
10.1.1 STP Terminology	101
10.1.2 How STP Works	102
10.1.3 STP Port States	102

10.2 STP Status	103
10.3 Configure STP	104
Chapter 11	
Bandwidth Control.....	107
11.1 Configuring Bandwidth Control	107
11.1.1 CIR and PIR	107
Chapter 12	
Broadcast Storm Control	109
12.1 Broadcast Storm Control Overview	109
12.2 Broadcast Storm Control Setup	109
Chapter 13	
Mirroring	111
13.1 Mirroring Overview	111
13.2 Port Mirroring Configuration	111
Chapter 14	
Link Aggregation	113
14.1 Link Aggregation Overview	113
14.1.1 Dynamic Link Aggregation	113
14.1.2 Link Aggregation ID	114
14.2 Link Aggregation Status	114
14.3 Link Aggregation Setup	115
Chapter 15	
Port Authentication.....	117
15.1 Port Authentication Overview	117
15.1.1 RADIUS	117
15.2 Configure Port Authentication	117
15.2.1 Activate IEEE 802.1x Security	118
15.2.2 Configuring RADIUS Server Settings	119
Chapter 16	
Port Security.....	121
16.1 Port Security Overview	121
16.2 Port Security Setup	121
Chapter 17	
Queuing Method.....	123
17.1 Queuing Method Overview	123
17.1.1 Strict Priority Queuing (SPQ)	123

17.1.2 Weighted Fair Scheduling (WFS)	124
17.2 Configuring Queuing	124
Chapter 18	
Classifier	127
18.1 Classifier Overview	127
18.2 Configuring a Classifier	127
18.3 Classifier Example	130
Chapter 19	
Policy	133
19.1 Policy Overview	133
19.1.1 DiffServ	133
19.1.2 DSCP and Per-Hop Behavior	133
19.2 Configuring a Policy	134
19.3 Policy Example	137
Chapter 20	
VLAN Stacking	139
20.1 VLAN Stacking Overview	139
20.1.1 VLAN Stacking Example	139
20.2 VLAN Stacking Port Roles	140
20.3 VLAN Tag Format	141
20.3.1 Frame Format	141
20.4 Configuring VLAN Stacking	142
Chapter 21	
Multicast	145
21.1 Multicast Overview	145
21.1.1 IP Multicast Addresses	145
21.1.2 IGMP Filtering	145
21.1.3 IGMP Snooping	145
21.2 Multicast Status	146
21.3 Multicast Setup	146
21.4 IGMP Filtering Profile	148
21.5 MVR Overview	149
21.5.1 Types of MVR Ports	150
21.5.2 MVR Modes	150
21.5.3 How MVR Works	150
21.6 General MVR Configuration	151
21.7 MVR Group Configuration	152
21.7.1 MVR Configuration Example	154

Chapter 22	
Differentiated Services	157
22.1 DiffServ Overview	157
22.1.1 DSCP and Per-Hop Behavior	157
22.1.2 DiffServ Network Example	157
22.2 Activating DiffServ	158
22.3 DSCP-to-IEEE802.1p Priority Setting	159
22.3.1 Configuring DSCP Setting	159
Part IV: Routing Protocol	161
Chapter 23	
Static Route	163
23.1 Configuring Static Route	163
Chapter 24	
DHCP Relay	165
24.1 DHCP Overview	165
24.1.1 DHCP Relay Agent Information	165
24.2 Configuring DHCP Relay	165
Part V: Management.....	167
Chapter 25	
Maintenance	169
25.1 The Maintenance Screen	169
25.2 Load Factory Default	170
25.3 Reboot System	170
25.4 Remote Device Upgrade	171
25.5 VDSL Chip Reset	172
25.6 Remote Device Reset	172
25.7 Firmware Upgrade	173
25.8 Restore a Configuration File	174
25.9 Backing Up a Configuration File	174
25.10 FTP Command Line	175
25.10.1 Filename Conventions	175
25.10.2 FTP Command Line Procedure	176
25.10.3 GUI-based FTP Clients	176
25.10.4 FTP Restrictions	177

Chapter 26	
Access Control.....	179
26.1 Access Control Overview	179
26.2 The Access Control Main Screen	179
26.3 About SNMP	180
26.3.1 Supported MIBs	181
26.3.2 SNMP Traps	181
26.3.3 Configuring SNMP	182
26.4 Setting Up Login Accounts	182
26.5 SSH Overview	184
26.6 How SSH works	184
26.7 SSH Implementation on the Switch	185
26.7.1 Requirements for Using SSH	185
26.7.2 SSH Login Example	185
26.8 Introduction to HTTPS	186
26.9 HTTPS Example	187
26.9.1 Internet Explorer Warning Messages	187
26.9.2 Netscape Navigator Warning Messages	188
26.9.3 The Main Screen	188
26.10 Service Access Control	189
26.11 Remote Management	190
Chapter 27	
Diagnostic.....	191
27.1 Diagnostic	191
Chapter 28	
Syslog.....	193
28.1 Syslog Overview	193
28.2 Syslog Setup	193
28.3 Syslog Server Setup	194
Chapter 29	
Cluster Management.....	197
29.1 Cluster Management Overview	197
29.2 Cluster Management Status	198
29.2.1 Cluster Member Switch Management	199
29.3 Configuring Cluster Management	200
Chapter 30	
MAC Table.....	203
30.1 MAC Table Overview	203
30.2 Viewing the MAC Table	204

Chapter 31	
ARP Table	205
31.1 ARP Table Overview	205
31.1.1 How ARP Works	205
31.2 Viewing the ARP Table	205
 Part VI: Commands, Troubleshooting and Specifications	207
 Chapter 32	
Introducing the Commands	209
32.1 Overview	209
32.1.1 Switch Configuration File	209
32.2 Accessing the CLI	210
32.2.1 Multiple Login	210
32.2.2 The Console Port	210
32.2.3 Telnet	211
32.2.4 SSH	212
32.3 The Login Screen	212
32.4 Command Syntax Conventions	212
32.5 Getting Help	213
32.5.1 List of Available Commands	213
32.5.2 Detailed Command Information	214
32.6 Changing the Password	214
32.7 Account Privilege Levels	215
32.8 Command Modes	215
32.9 Using Command History	216
32.10 Saving Your Configuration	217
32.10.1 Logging Out	217
32.11 Command Summary	217
32.11.1 User Mode	217
32.11.2 Enable Mode	218
32.11.3 General Configuration Mode	223
32.11.4 interface Commands	233
32.11.5 mvr Commands	236
32.11.6 vdsl-alarmprofile Commands	237
32.11.7 vdsl-profile Commands	238
32.11.8 vlan Commands	240
 Chapter 33	
Command Examples.....	243
33.1 Overview	243

33.2 show Commands	243
33.2.1 show interface	243
33.2.2 show ip	244
33.2.3 show logging	244
33.2.4 show mac address-table all	244
33.2.5 show multi-login	245
33.2.6 show system-information	245
33.2.7 show vdsl-alarmprofile	246
33.2.8 show vdsl-profile	246
33.3 ping	247
33.4 traceroute	248
33.5 Enabling RSTP	249
33.6 vdsl-port Command	249
33.7 Configuration File Maintenance	249
33.7.1 Backing up Configuration	249
33.7.2 Restoring Configuration	250
33.7.3 Resetting to the Factory Default	250
33.8 no Command Examples	251
33.8.1 no mirror port	251
33.8.2 no https timeout	251
33.8.3 no trunk	251
33.8.4 no port-access-authenticator	252
33.8.5 no ssh	252
33.9 interface Commands	253
33.9.1 interface port-channel	253
33.9.2 bpdu-control	253
33.9.3 broadcast-limit	254
33.9.4 bandwidth-limit	254
33.9.5 mirror	255
33.9.6 gvrp	255
33.9.7 ingress-check	256
33.9.8 frame-type	256
33.9.9 egress set	256
33.9.10 qos priority	257
33.9.11 name	257
33.9.12 speed-duplex	258
Chapter 34	
IEEE 802.1Q Tagged VLAN Commands	259
34.1 Configuring Tagged VLAN	259
34.2 Global VLAN1Q Tagged VLAN Configuration Commands	260
34.2.1 GARP Status	260
34.2.2 GARP Timer	260

34.2.3 GVRP Timer	261
34.2.4 Enable GVRP	261
34.2.5 Disable GVRP	261
34.3 Port VLAN Commands	261
34.3.1 Set Port VID	261
34.3.2 Set Acceptable Frame Type	262
34.3.3 Enable or Disable Port GVRP	262
34.3.4 Modify Static VLAN	262
34.3.5 Forwarding Process Example	263
34.4 Delete VLAN ID	264
34.5 Enable VLAN	264
34.6 Disable VLAN	264
34.7 Show VLAN Setting	264
Chapter 35	
Troubleshooting.....	267
35.1 Problems Starting Up the Switch	267
35.2 Problems Accessing the Switch	267
35.3 Problem with the VDSL Connection	268
35.3.1 Pop-up Windows, JavaScripts and Java Permissions	268
35.4 Problems with the Password	273
Chapter 36	
Product Specifications	275
 Part VII: Appendices and Index	 283
Appendix A IP Addresses and Subnetting	285
Appendix B Legal Information	295
Appendix C Customer Support.....	299
Index.....	303

Contents Overview

Introduction	29
Getting to Know Your Switch	31
Hardware Installation	35
Hardware Overview	37
Status and Basic	43
The Web Configurator	45
System Status and Port Statistics	53
Basic Setting	63
Advanced	85
VLAN	87
Static MAC Forward Setup	97
Filtering	99
Spanning Tree Protocol	101
Bandwidth Control	107
Broadcast Storm Control	109
Mirroring	111
Link Aggregation	113
Port Authentication	117
Port Security	121
Queuing Method	123
Classifier	127
Policy	133
VLAN Stacking	139
Multicast	145
Differentiated Services	157
Routing Protocol	161
Static Route	163
DHCP Relay	165
Management	167
Maintenance	169
Access Control	179
Diagnostic	191
Syslog	193

Cluster Management	197
MAC Table	203
ARP Table	205
Commands, Troubleshooting and Specifications	207
Introducing the Commands	209
Command Examples	243
IEEE 802.1Q Tagged VLAN Commands	259
Troubleshooting	267
Product Specifications	275
Appendices and Index	283

List of Figures

Figure 1 MTU Application	32
Figure 2 Curbside Application	32
Figure 3 Attaching the Mounting Brackets	36
Figure 4 Mounting the Switch on a Rack	36
Figure 5 Front Panel	37
Figure 6 Transceiver Installation Example	39
Figure 7 Installed Transceiver	39
Figure 8 Opening the Transceiver's Latch Example	39
Figure 9 Transceiver Removal Example	39
Figure 10 Web Configurator: Login	45
Figure 11 Web Configurator Home Screen (Status)	46
Figure 12 Change Administrator Login Password	50
Figure 13 Resetting the Switch: Via the Console Port	52
Figure 14 Web Configurator: Logout Screen	52
Figure 15 Status	53
Figure 16 Status: VDSL Summary	55
Figure 17 Status: VDSL Port Details	55
Figure 18 Status: Port Details	59
Figure 19 System Info	64
Figure 20 General Setup	66
Figure 21 Switch Setup	68
Figure 22 IP Setup	70
Figure 23 Port Setup	73
Figure 24 VDSL Profile Setup	78
Figure 25 VDSL Alarm Profile Setup	81
Figure 26 PSD-Frequency Example	82
Figure 27 VDSL PSD Profile Setup	83
Figure 28 Port VLAN Trunking	89
Figure 29 Switch Setup: Select VLAN Type	89
Figure 30 VLAN > VLAN Status	90
Figure 31 VLAN > Static VLAN	91
Figure 32 VLAN > VLAN Port Setting	92
Figure 33 Port Based VLAN Setup (All Connected)	94
Figure 34 Port Based VLAN Setup (Port Isolation)	95
Figure 35 Static MAC Forwarding	97
Figure 36 Filtering	99
Figure 37 Spanning Tree Protocol Status	103
Figure 38 Spanning Tree Protocol > Configuration	104

Figure 39 Bandwidth Control	108
Figure 40 Broadcast Storm Control	109
Figure 41 Mirroring	111
Figure 42 Link Aggregation Control Protocol Status	114
Figure 43 Link Aggregation Control Protocol > Configuration	115
Figure 44 RADIUS Server	117
Figure 45 Port Authentication	118
Figure 46 Port Authentication > 802.1x	118
Figure 47 Port Authentication > RADIUS	119
Figure 48 Port Security	121
Figure 49 Queuing Method	124
Figure 50 Classifier	128
Figure 51 Classifier Example	131
Figure 52 Policy	135
Figure 53 Policy Example	138
Figure 54 VLAN Stacking Example	140
Figure 55 VLAN Stacking	142
Figure 56 Multicast Status	146
Figure 57 Multicast	147
Figure 58 Multicast > IGMP Filtering Profile	148
Figure 59 MVR Network Example	149
Figure 60 MVR Multicast Television Example	150
Figure 61 MVR	151
Figure 62 MVR > Group Configuration	153
Figure 63 MVR Configuration Example	154
Figure 64 MVR Configuration Example	154
Figure 65 MVR Group Configuration Example	155
Figure 66 DiffServ: Differentiated Service Field	157
Figure 67 DiffServ Network Example	158
Figure 68 DiffServ	158
Figure 69 DiffServ > DSCP Setting	159
Figure 70 Static Routing	163
Figure 71 DHCP Relay	166
Figure 72 Maintenance	169
Figure 73 Load Factory Default: Conformation	170
Figure 74 Load Factory Default: Start	170
Figure 75 Reboot System: Confirmation	170
Figure 76 Reboot System: Start	171
Figure 77 Maintenance: Remote Device Upgrade	171
Figure 78 Maintenance: VDSL Chip Reset	172
Figure 79 Maintenance: Remote Device Reset	173
Figure 80 Firmware Upgrade	174
Figure 81 Restore Configuration	174

Figure 82 Backup Configuration	175
Figure 83 Access Control	180
Figure 84 SNMP Management Model	180
Figure 85 Access Control: SNMP	182
Figure 86 Access Control: Logins	183
Figure 87 SSH Communication Example	184
Figure 88 How SSH Works	184
Figure 89 SSH Login Example	186
Figure 90 HTTPS Implementation	187
Figure 91 Security Alert Dialog Box (Internet Explorer)	187
Figure 92 Security Certificate 1 (Netscape)	188
Figure 93 Security Certificate 2 (Netscape)	188
Figure 94 Example: Lock Denoting a Secure Connection	189
Figure 95 Access Control: Service Access Control	189
Figure 96 Access Control: Remote Management	190
Figure 97 Diagnostic	191
Figure 98 Syslog Setup	194
Figure 99 Syslog Server Setup	195
Figure 100 Clustering Application Example	197
Figure 101 Cluster Management Status	198
Figure 102 Cluster Management: Cluster Member Web Configurator Screen	199
Figure 103 Example: Uploading Firmware to a Cluster Member Switch	199
Figure 104 Clustering Management Configuration	200
Figure 105 MAC Table Flowchart	203
Figure 106 MAC Table	204
Figure 107 ARP Table	206
Figure 108 Pop-up Blocker	269
Figure 109 Internet Options	269
Figure 110 Internet Options	270
Figure 111 Pop-up Blocker Settings	270
Figure 112 Internet Options	271
Figure 113 Security Settings - Java Scripting	272
Figure 114 Security Settings - Java	272
Figure 115 Java (Sun)	273
Figure 116 Hardware Telco-50 Pin Assignments	279
Figure 117 Telco-50 Cable VDSL Telco-50 Pin Assignments	280
Figure 118 Telco-50 Cable POTS/ISDN Telco-50 Pin Assignments	280
Figure 119 Console Cable DB-9 End Pin Layout	281
Figure 120 Network Number and Host ID	286
Figure 121 Subnetting Example: Before Subnetting	288
Figure 122 Subnetting Example: After Subnetting	289
Figure 123 Conflicting Computer IP Addresses Example	293
Figure 124 Conflicting Computer IP Addresses Example	293

Figure 125 Conflicting Computer and Router IP Addresses Example	294
---	-----

List of Tables

Table 1 Front Panel	37
Table 2 LEDs	40
Table 3 Navigation Panel Sub-links Overview	47
Table 4 Web Configurator Screen Sub-links Details	48
Table 5 Navigation Panel Links	48
Table 6 Status	54
Table 7 Status: VDSL Port Details	56
Table 8 Status: Port Details	60
Table 9 System Info	64
Table 10 General Setup	66
Table 11 Switch Setup	68
Table 12 IP Setup	71
Table 13 Port Setup	73
Table 14 VDSL Profile Setup	78
Table 15 VDSL Alarm Profile Setup	81
Table 16 VDSL PSD Profile Setup	83
Table 17 IEEE 802.1Q Terminology	88
Table 18 VLAN > VLAN Status	90
Table 19 VLAN > Static VLAN	91
Table 20 VLAN > VLAN Port Setting	92
Table 21 Port Based VLAN Setup	95
Table 22 Static MAC Forwarding	97
Table 23 Filtering	99
Table 24 STP Path Costs	101
Table 25 STP Port States	102
Table 26 Spanning Tree Protocol Status	103
Table 27 Spanning Tree Protocol > Configuration	104
Table 28 Bandwidth Control	108
Table 29 Broadcast Storm Control	109
Table 30 Mirroring	112
Table 31 Link Aggregation ID: Local Switch	114
Table 32 Link Aggregation ID: Peer Switch	114
Table 33 Link Aggregation Control Protocol Status	114
Table 34 Link Aggregation Control Protocol > Configuration	115
Table 35 Port Authentication > 802.1x	118
Table 36 Port Authentication > RADIUS	119
Table 37 Port Security	122
Table 38 Physical Queue Priority	123

Table 39 Queuing Method	125
Table 40 Classifier	128
Table 41 Common Ethernet Type Number	130
Table 42 Common Protocol Port Number	130
Table 43 Policy	136
Table 44 VLAN Tag Format	141
Table 45 Single and Double Tagged 802.11Q Frame Format	141
Table 46 IEEE 802.1Q Frame	141
Table 47 VLAN Stacking	142
Table 48 Multicast Status	146
Table 49 Multicast	147
Table 50 Multicast > IGMP Filtering Profile	149
Table 51 MVR	152
Table 52 MVR > Group Configuration	153
Table 53 DiffServ	158
Table 54 Default DSCP-IEEE802.1p Mapping	159
Table 55 DiffServ > DSCP Setting	159
Table 56 Static Routing	163
Table 57 DHCP Relay	166
Table 58 Maintenance	169
Table 59 Switch Hardware Version	173
Table 60 Filename Conventions	175
Table 61 Access Control Overview	179
Table 62 SNMP Commands	181
Table 63 SNMP Traps	181
Table 64 Access Control: SNMP	182
Table 65 Access Control: Logins	183
Table 66 Access Control: Service Access Control	189
Table 67 Access Control: Remote Management	190
Table 68 Diagnostic	191
Table 69 Syslog Severity Levels	193
Table 70 Syslog	194
Table 71 Syslog Server Setup	195
Table 72 ZyXEL Clustering Management Specifications	197
Table 73 Cluster Management Status	198
Table 74 FTP Upload to Cluster Member Example	200
Table 75 Clustering Management Configuration	201
Table 76 MAC Table	204
Table 77 ARP Table	206
Table 78 Command Interpreter Mode Summary	215
Table 79 Command Summary: User Mode	217
Table 80 Command Summary: Enable Mode	218
Table 81 Command Summary: Configuration Mode	223

Table 82 interface port-channel Commands	233
Table 83 mvr Commands	236
Table 84 vdsl-alarmprofile Commands	237
Table 85 vdsl-profile Commands	238
Table 86 vlan Commands	240
Table 87 Troubleshooting the Start-Up of Your Switch	267
Table 88 Troubleshooting Accessing the Switch	267
Table 89 Troubleshooting VDSL Connection	268
Table 90 Troubleshooting the Password	273
Table 91 Product Specifications	275
Table 92 CO Impedance Splitter Board Specifications	277
Table 93 Hardware Telco-50 Pin Assignments	278
Table 94 Hardware Telco-50 Connector Port and Pin Numbers	279
Table 95 Console Port Pin Assignments	281
Table 96 IP Address Network Number and Host ID Example	286
Table 97 Subnet Masks	287
Table 98 Maximum Host Numbers	287
Table 99 Alternative Subnet Mask Notation	287
Table 100 Subnet 1	289
Table 101 Subnet 2	290
Table 102 Subnet 3	290
Table 103 Subnet 4	290
Table 104 Eight Subnets	290
Table 105 24-bit Network Number Subnet Planning	291
Table 106 16-bit Network Number Subnet Planning	291

PART I

Introduction

Getting to Know Your Switch (31)

Hardware Installation (35)

Hardware Overview (37)

Getting to Know Your Switch

This chapter introduces the main features and applications of the switch.

1.1 Introduction

The VES-1616F-3x series switches are stand-alone layer-2 VDSL (Very High Speed Digital Subscriber Line) over POTS/ISDN switches.

The series consist of the following models at the time of writing.

- VES-1616F-34 (VDSL1),
- VES-1616F-34 (VDSL2),
- VES-1616F-35 (VDSL1) and
- VES-1616F-35 (VDSL2).

Use the `show hardware-version` command to check whether your device is a VDSL1 switch (100100, or 10050) or VDSL2 switch (5030). See Chapter 32 on page 211 for more information.

VDSL2 is the second generation of the VDSL (which is currently denoted VDSL1) standard.



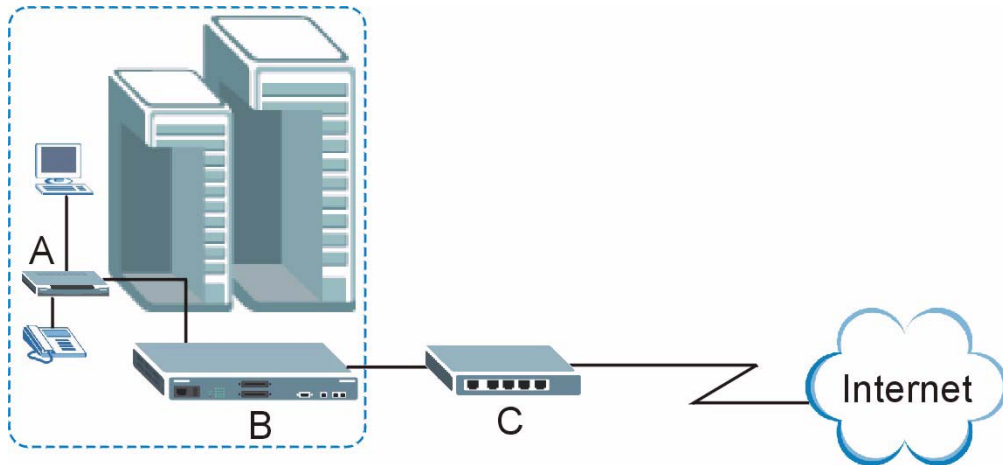
You can only upload the firmware of the same VDSL standard as your Switch model.

1.2 Applications

This section shows the main applications for the switch:

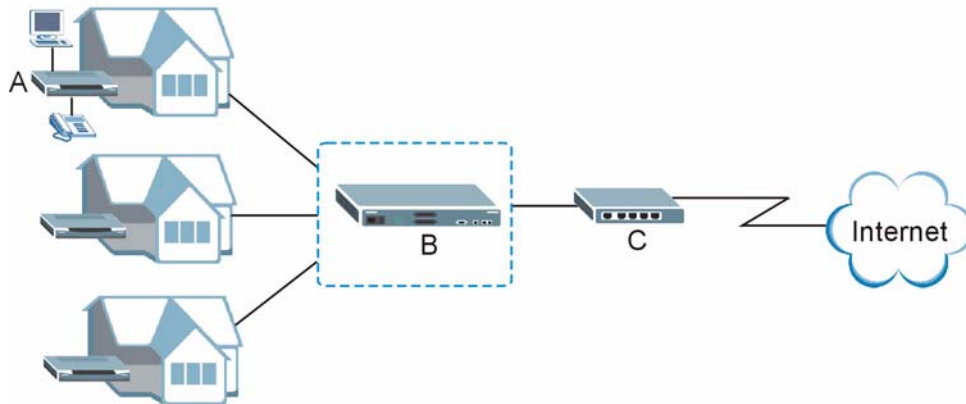
1.2.1 MTU Application

The following diagram depicts a typical application of the Switch (labeled **B**) with the VDSL modems (labeled **A**), in a large residential building, or multiple tenant unit (MTU), that leverages existing phone line wiring to provide Internet access to all tenants. Note that VDSL service can coexist with voice service on the same line. The Switch is connected to a backbone switch (labeled **C**) using an Ethernet cable or a fiber-optic cable. The fiber connection allows distances of up to several kilometers (depending on your transceivers). The Ethernet connection is a suitable link for distances up to 100 meters (328 feet).

Figure 1 MTU Application

1.2.2 Curbside Application

You could place the Switch outdoors (in a street cabinet for example) in residential areas that are too far away from the ISP (Internet Service Provider) to receive DSL services. Residents only need to be within range of the Switch (not the ISP) to receive high-speed VDSL Internet access, and have enough bandwidth for data, voice, and video services. In the following example, the Switch (labeled **B**) is placed a considerable distance from the ISP and connected to a backbone switch (labeled **C**).

Figure 2 Curbside Application

1.3 Ways to Manage the Switch

Use any of the following methods to manage the Switch.

- **Web Configurator.** This is recommended for everyday management of the Switch using a (supported) web browser. See [Chapter 4 on page 45](#).
- **Command Line Interface.** Line commands offer an alternative to the Web Configurator and may be necessary to configure advanced features. See [Chapter 32 on page 209](#).

- FTP. Use File Transfer Protocol for firmware upgrades and configuration backup/restore. See [Chapter 25 on page 169](#).
- SNMP. The device can be monitored and/or managed by an SNMP manager. See [Chapter 26 on page 179](#).

1.4 Good Habits for Managing the Switch

Do the following things regularly to make the Switch more secure and to manage the Switch more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the Switch to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the Switch. You could simply restore your last configuration.

Hardware Installation

This chapter shows you how to install the switch.



Do NOT block the ventilation holes. Leave space between devices when stacking.

For proper ventilation, allow at least 4 inches (10 cm) of clearance at the front and 3.4 inches (8 cm) at the back of the switch. This is especially important for enclosed rack installations.

2.1 Mounting the Switch on a Rack

This section lists the rack mounting requirements and precautions and describes the installation steps.

2.1.1 Rack-mounted Installation Requirements

- Two mounting brackets.
- Eight M3 flat head screws and a #2 Philips screwdriver.
- Four M5 flat head screws and a #2 Philips screwdriver.



Failure to use the proper screws may damage the unit.

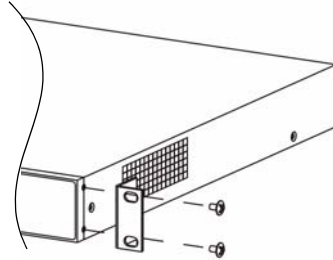
2.1.1.1 Precautions

- Make sure the rack will safely support the combined weight of all the equipment it contains.
- Make sure the position of the switch does not make the rack unstable or top-heavy. Take all necessary precautions to anchor the rack securely before installing the unit.

2.1.2 Attaching the Mounting Brackets to the Switch

- 1 Position a mounting bracket on one side of the switch, lining up the four screw holes on the bracket with the screw holes on the side of the switch.

Figure 3 Attaching the Mounting Brackets

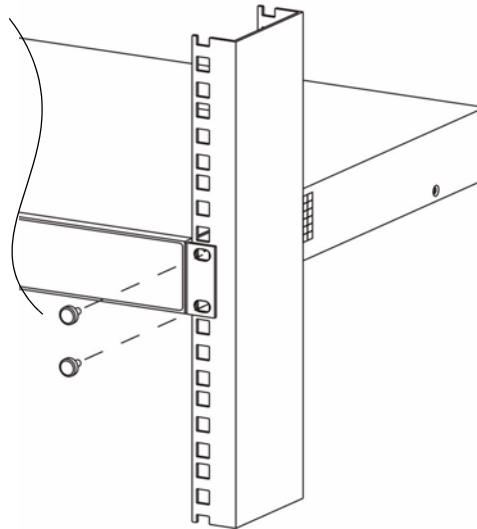


- 2 Using a #2 Philips screwdriver, install the M3 flat head screws through the mounting bracket holes into the switch.
- 3 Repeat steps 1 and 2 to install the second mounting bracket on the other side of the switch.
- 4 You may now mount the switch on a rack. Proceed to the next section.

2.1.3 Mounting the Switch on a Rack

- 1 Position a mounting bracket (that is already attached to the switch) on one side of the rack, lining up the two screw holes on the bracket with the screw holes on the side of the rack.

Figure 4 Mounting the Switch on a Rack



- 2 Using a #2 Philips screwdriver, install the M5 flat head screws through the mounting bracket holes into the rack.
- 3 Repeat steps 1 and 2 to attach the second mounting bracket on the other side of the rack.

Hardware Overview

This chapter describes the front panel and rear panel of the switch and shows you how to make the hardware connections.

3.1 Front Panel Connection

The front panel contains switch LEDs and all the network ports and port connections.

Figure 5 Front Panel



The following table describes the port labels on the front panel.

Table 1 Front Panel

PORT	DESCRIPTION
POTS/ISDN LINE (Optional)	This Telco-50 port connects to the central office or a PBX.
VDSL LINE	This Telco-50 port connects to the user (subscriber) VDSL equipment.
17, 18	These Gigabit/mini-GBIC uplink ports allow you to connect to any other switches.
CONSOLE	The console port is for local management.
MGMT	This RJ-45 port is for local management.

3.1.1 VDSL and POTS Connections

Connect the lines from the user equipment (VDSL modem) to the **VDSL LINE** port and the lines from the central office switch or PBX (Private Branch Exchange) to the **POTS/ISDN LINE** port. Make sure that the VDSL LINE Telco-50 cable and the POTS/ISDN LINE Telco-50 cable are not shorted on the MDF (Main Distribution Frame).

The line from the user carries both the VDSL and the voice signals. For each line, the switch has a built-in splitter that separates the high frequency VDSL signal from the voice band signal and feeds the VDSL signal to the switch, while the voice band signal is diverted to the **POTS/ISDN LINE** port.

Refer to [Appendix on page 275](#) for Telco50 pin assignments.

3.1.2 Gigabit Ethernet Ports

There are two pairs of Gigabit Ethernet/mini-GBIC ports. The mini-GBIC ports have priority over the Gigabit ports. This means that if a mini-GBIC port and the corresponding Gigabit port are connected at the same time, the Gigabit port will be disabled. The speed of the Gigabit Ethernet/mini-GBIC ports can be 100Mbps or 1000Mbps and the duplex mode can be half duplex (at 100 Mbps) or full duplex. The ports are auto-negotiating and auto-crossover.

An auto-negotiating port can detect and adjust to the optimum Ethernet speed (10/100/1000Mbps) and duplex mode (full duplex or half duplex) of the connected device.

An auto-crossover (auto-MDI/MDI-X) port automatically works with a straight-through or crossover Ethernet cable.

3.1.2.1 Default Ethernet Settings

The factory default negotiation settings for the Ethernet ports on the switch are:

- Speed: Auto
- Duplex: Auto
- Flow control: on
- Trunking: Disabled

3.1.3 Mini-GBIC Slots

These are slots for mini-GBIC (Gigabit Interface Converter) transceivers. A transceiver is a single unit that houses a transmitter and a receiver. The switch does not come with transceivers. You must use transceivers that comply with the Small Form-factor Pluggable (SFP) Transceiver MultiSource Agreement (MSA). See the SFF committee's INF-8074i specification Rev 1.0 for details.

The mini-GBIC ports have priority over the Gigabit ports. This means that if a mini-GBIC port and the corresponding Gigabit port are connected at the same time, the Gigabit port will be disabled.

You can change transceivers while the switch is operating. You can use different transceivers to connect to Ethernet switches with different types of fiber-optic connectors.

- Type: SFP connection interface
- Connection speed: 1 Gigabit per second (Gbps)

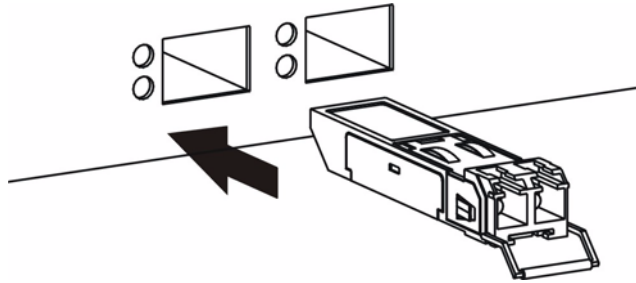


To avoid possible eye injury, do NOT look into an operating fiber-optic module's connectors.

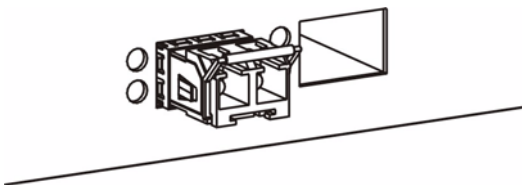
3.1.3.1 Transceiver Installation

Use the following steps to install a mini GBIC transceiver (SFP module).

- 1 Insert the transceiver into the slot with the exposed section of PCB board facing down.

Figure 6 Transceiver Installation Example

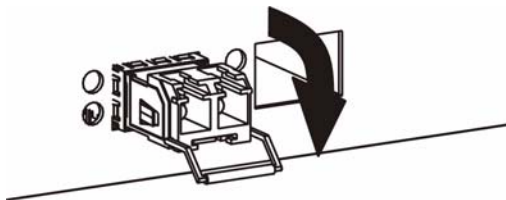
- 2 Press the transceiver firmly until it clicks into place.
- 3 The switch automatically detects the installed transceiver. Check the LEDs to verify that it is functioning properly.

Figure 7 Installed Transceiver

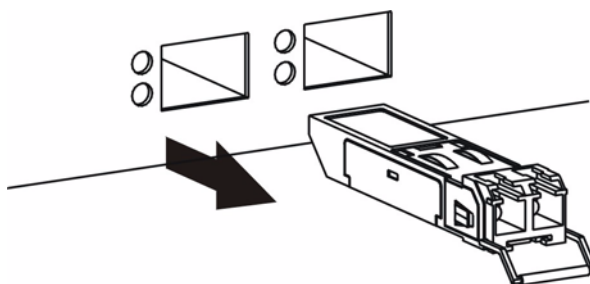
3.1.3.2 Transceiver Removal

Use the following steps to remove a mini GBIC transceiver (SFP module).

- 1 Open the transceiver's latch (latch styles vary).

Figure 8 Opening the Transceiver's Latch Example

- 2 Pull the transceiver out of the slot.

Figure 9 Transceiver Removal Example

3.1.4 Console Port

For local management, you can use a computer with terminal emulation software configured to the following parameters:

- VT100 terminal emulation
- 9600 bps
- No parity, 8 data bits, 1 stop bit
- No flow control

Connect the male 9-pin end of the console cable to the console port of the switch. Connect the female end to a serial port (COM1, COM2 or other COM port) of your computer.

3.1.5 Power Connector

Make sure you are using the correct power source as shown on the panel.



Make sure that no objects obstruct the airflow of the fans.

3.2 LEDs

The LEDs are located on the front panel. The following table describes the LEDs on the front panel.

Table 2 LEDs

LED	COLOR	STATUS	DESCRIPTION
PWR	Green	On	The system is turned on.
		Off	The system is off.
SYS	Green	Blinking	The system is rebooting and performing self-diagnostic tests.
		On	The system is on and functioning properly.
		Off	The power is off or the system is not ready or malfunctioning.
ALM	Red	On	There is a hardware failure (abnormal temperature, voltage or fan speeds).
		Off	The system is functioning normally.
VDSL	Green	On	The link to a VDSL line is up and the system is transmitting or receiving to/from a VDSL link.
		Off	The link to a VDSL line is down.
Gigabit Ports			
LNK/ACT	Green	On	The link to a 10 Mbps Ethernet network is up. The link to a 1000 Mbps Ethernet network is up if the amber LED is on at the same time.
		Blinking	The port is receiving or transmitting data at 10 Mbps
	Amber	On	The link to a 100 Mbps Ethernet network is up. The link to a 1000 Mbps Ethernet network is up if the green LED is on at the same time.
		Blinking	The port is receiving or transmitting data at 100 Mbps.
		Off	The link to an Ethernet network is down.
Mini-GBIC Slots			

Table 2 LEDs (continued)

LED	COLOR	STATUS	DESCRIPTION
LNK	Green	On	The port has a successful connection.
		Off	No Ethernet device is connected to this port.
ACT	Green	Blinking	The port is sending or receiving data.
		Off	The port is not sending or receiving data.
MGMT			
	Green	On	The link to a 10 Mbps Ethernet network is up.
		Blinking	The port is receiving or transmitting data at 10 Mbps.
	Amber	On	The link to a 100 Mbps Ethernet network is up.
		Blinking	The port is receiving or transmitting data at 100 Mbp.
		Off	The link to an Ethernet network is down.

PART II

Status and Basic

[The Web Configurator \(45\)](#)

[System Status and Port Statistics \(53\)](#)

[Basic Setting \(63\)](#)

The Web Configurator

This section introduces the configuration and functions of the web configurator.

4.1 Introduction

The web configurator is an HTML-based management interface that allows easy switch setup and management via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

4.2 System Login

- 1 Start your web browser.
- 2 Type “http://” and the IP address of the switch (for example, the default for the management port is 192.168.0.1 and for the switch port is 192.168.1.1) in the **Location** or **Address** field. Press [ENTER].
- 3 The login screen appears. The default username is **admin** and associated default password is **1234**. The date and time display as shown if you have not configured a time server nor manually entered a time and date in the **General Setup** screen.

Figure 10 Web Configurator: Login



- 4 Click **OK** to view the first web configurator screen.

4.3 The Status Screen

The **Status** screen is the first screen that displays when you access the web configurator. The following figure shows the navigating components of a web configurator screen.

Figure 11 Web Configurator Home Screen (Status)

ZyXEL Status Logout Help

MENU
 Basic Setting
 Advanced Application
 Routing Protocol
 Management

Status [VDSL Summary](#)

System Up Time : 0:18:14

Port	PayLoad Rate	State	Tx KB/s	Rx KB/s	Up Time	Retrain
1	0/0	Standby	0	0	0:00:00	Retrain
2	0/0	Standby	0	0	0:00:00	Retrain
3	0/0	Standby	0	0	0:00:00	Retrain
4	0/0	Standby	0	0	0:00:00	Retrain
5	0/0	Standby	0	0	0:00:00	Retrain
6	0/0	Standby	0	0	0:00:00	Retrain
7	0/0	Standby	0	0	0:00:00	Retrain
8	0/0	Standby	0	0	0:00:00	Retrain
9	0/0	Standby	0	0	0:00:00	Retrain
10	0/0	Standby	0	0	0:00:00	Retrain
11	0/0	Standby	0	0	0:00:00	Retrain
12	0/0	Standby	0	0	0:00:00	Retrain
13	0/0	Standby	0	0	0:00:00	Retrain
14	0/0	Standby	0	0	0:00:00	Retrain
15	0/0	Standby	0	0	0:00:00	Retrain
16	0/0	Standby	0	0	0:00:00	Retrain

Port	Link	State	LACP	TxPkts	RxPkts	Tx KB/s	Rx KB/s	Up Time
17	Down	STOP	Disabled	0	0	0.0	0.0	0:00:00
18	100M/F	FORWARDING	Disabled	741	2453	17.428	2.794	0:18:03

Poll Interval(s) Port

In the navigation panel, click a main link to reveal a list of submenu links.

Table 3 Navigation Panel Sub-links Overview

BASIC SETTING	ADVANCED APPLICATION	ROUTING PROTOCOL	MANAGEMENT
<div><div>MENU</div><div>Basic Setting</div><div>Advanced Application</div><div>Routing Protocol</div><div>Management</div><div>System Info</div><div>General Setup</div><div>Switch Setup</div><div>IP Setup</div><div>Port Setup</div><div>VDSL Profile Setup</div><div>VDSL Alarm Profile Setup</div><div>VDSL PSD Profile Setup</div></div>	<div><div>MENU</div><div>Basic Setting</div><div>Advanced Application</div><div>Routing Protocol</div><div>Management</div><div>VLAN</div><div>Static MAC Forwarding</div><div>Filtering</div><div>Spanning Tree Protocol</div><div>Bandwidth Control</div><div>Broadcast Storm Control</div><div>Mirroring</div><div>Link Aggregation</div><div>Port Authentication</div><div>Port Security</div><div>Queueing Method</div><div>Classifier</div><div>Policy Rule</div><div>VLAN Stacking</div><div>Multicast</div><div>DiffServ</div></div>	<div><div>MENU</div><div>Basic Setting</div><div>Advanced Application</div><div>Routing Protocol</div><div>Management</div><div>Static Routing</div><div>DHCP Relay</div></div>	<div><div>MENU</div><div>Basic Setting</div><div>Advanced Application</div><div>Routing Protocol</div><div>Management</div><div>Maintenance</div><div>Access Control</div><div>Diagnostic</div><div>Syslog</div><div>Cluster Management</div><div>MAC Table</div><div>ARP Table</div></div>

The following table lists the various web configurator screens within the sub-links

Table 4 Web Configurator Screen Sub-links Details

BASIC SETTING	ADVANCED APPLICATION	ROUTING APPLICATION	MANAGEMENT
System Info General Setup Switch Setup IP Setup Port Setup VDSL Profile Setup VDSL Alarm Profile Setup VDSL PSD Profile Setup	VLAN Status VLAN Port Setting Static VLAN Static MAC Forwarding Filtering Spanning Tree Protocol Status Spanning Tree Protocol Configuration Bandwidth Control Broadcast Storm Control Mirroring Link Aggregation Status Link Aggregation Configuration Port Authentication RADIUS 802.1x Port Security Queuing Method Classifier Policy Rule VLAN Stacking Multicast IGMP Filtering Profile Multicast Status MVR Group Configuration DiffServ DSCP Setting	Static Routing DHCP Relay	Maintenance Remote Device Upgrade VDSL Chip Reset Remote Device Reset Firmware Upgrade Restore Configuration Backup Configuration Load Factory Default Reboot System Access Control SNMP Logins Service Access Control Remote Management Diagnostic Syslog Cluster Management MAC Table ARP Table

The following table describes the links in the navigation panel.

Table 5 Navigation Panel Links

LINK	DESCRIPTION
Basic Settings	
System Info	This link takes you to a screen that displays general system and hardware monitoring information.
General Setup	This link takes you to a screen where you can configure general identification information about the switch.
Switch Setup	This link takes you to a screen where you can set up global switch parameters such as VLAN type, MAC address learning, IGMP snooping, GARP and priority queues.
IP Setup	This link takes you to a screen where you can configure the IP address, subnet mask (necessary for switch management) and DNS (domain name server).
Port Setup	This link takes you to screens where you can configure settings for individual switch ports.
VDSL Profile Setup	This link takes you to a screen where you can configure VDSL profiles.

Table 5 Navigation Panel Links (continued)

LINK	DESCRIPTION
VDSL Alarm Profile Setup	This link takes you to a screen where you can configure VDSL alarm profiles to apply to the VDSL lines.
VDSL PSD Profile Setup	This link takes you to a screen where you can configure VDSL PSD profiles to apply to the VDSL lines.
Advanced Application	
VLAN	This link takes you to screens where you can configure port-based or 802.1Q VLAN (depending on what you configured in the Switch Setup screen).
Static MAC Forwarding	This link takes you to screens where you can configure static MAC addresses for a port. These static MAC addresses do not age out.
Filtering	This link takes you to a screen to set up filtering rules.
Spanning Tree Protocol	This link takes you to screens where you can configure the STP/RSTP to prevent network loops.
Bandwidth Control	This link takes you to screens where you can cap the maximum bandwidth allowed from specified source(s) to specified destination(s).
Broadcast Storm Control	This link takes you to a screen to set up broadcast filters.
Mirroring	This link takes you to screens where you can copy traffic from one port or ports to another port in order that you can examine the traffic from the first port without interference
Link Aggregation	This link takes you to a screen where you can logically aggregate physical links to form one logical, higher-bandwidth link.
Port Authentication	This link takes you to a screen where you can configure RADIUS (Remote Authentication Dial-In User Service), a protocol for user authentication that allows you to use an external server to validate an unlimited number of users.
Port Security	This link takes you to a screen where you can activate MAC address learning and set the maximum number of MAC addresses to learn on a port.
Queuing Method	This link takes you to a screen where you can configure SPQ or WFQ with associated queue weights for each port.
Classifier	This link takes you to a screen where you can configure the switch to group packets based on the specified criteria.
Policy Rule	This link takes you to a screen where you can define actions on classified traffic flows.
VLAN Stacking	This link takes you to a screen where you can configure VLAN stacking.
Multicast	This link takes you to screens where you can configure multicast functions (such as IGMP) on the switch.
MVR	This link takes you to screens where you can configure MVR (Multicast VLAN Registration).
DiffServ	This link takes you to screens where you can enable DiffServ, configure marking rules and set DSCP-to-IEEE802.1p mappings.
Routing Protocol	
Static Routing	This link takes you to screens where you can configure static routes. A static route defines how the switch should forward traffic by configuring the TCP/IP parameters manually.
DHCP Relay	This link takes you to a screen where you can configure the DHCP relay settings for the network on the switch.
Management	

Table 5 Navigation Panel Links (continued)

LINK	DESCRIPTION
Maintenance	This link takes you to screens where you can perform firmware and configuration file maintenance as well as reboot the system.
Access Control	This link takes you to screens where you can change the system login password and configure SNMP and remote management.
Diagnostic	This link takes you to screens where you can view system logs and test port(s).
Syslog	This link takes you to screens where you can enable syslog logging and configure syslog server settings.
Cluster Management	This link takes you to a screen where you can configure clustering management and view its status.
MAC Table	This link takes you to a screen where you can view the MAC addresses (and types) of devices attached to what ports and VLAN IDs.
ARP Table	This link takes you to a screen where you can view the MAC addresses – IP address resolution table.

4.3.1 Change Your Password

After you log in for the first time, it is recommended you change the default administrator password. Click **Management > Access Control > Logins** to display the next screen.

Figure 12 Change Administrator Login Password

Logins Access Control

Administrator

Old Password

New Password

Retype to confirm

Please record your new password whenever you change it. The system will lock you out if you have forgotten your password.

Edit Logins

Login	User Name	Password	Retype to confirm
1	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>

4.4 Switch Lockout

You are locked out from managing the switch if another administrator is currently logged in. You must wait until he/she has logged out before you can log in.

Any of the following could also lock you and others out from using in-band management (managing through the data ports).

Moreover, you could lock yourself (and all others) out from the switch by:

- 1 Deleting the management VLAN (default is VLAN 1).

- 2 Deleting all port-based VLANs with the CPU port as a member. The “CPU port” is the management port of the switch.
- 3 Incorrectly configuring the access control settings. This could also lock you out from performing out-of-band management (managing through the console port or management port).
- 4 Disabling all ports.
- 5 Assigning minimum bandwidth to the CPU port. If you limit bandwidth to the CPU port, you may find that the switch performs sluggishly or not at all.



Be careful not to lock yourself and others out of the switch.

4.5 Resetting the Switch

If you lock yourself (and others) out of the switch, you can try using out-of-band management. If you still cannot correct the situation or forgot the password, you will need to reload the factory-default configuration file.

4.5.1 Reload the Configuration File

Uploading the factory-default configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all previous configurations and the speed of the console port will be reset to the default of 9600bps with 8 data bit, no parity, one stop bit and flow control set to none. The password will also be reset to “1234” and the IP address to 192.168.1.1.

To upload the configuration file, do the following:

- 1 Connect to the console port using a computer with terminal emulation software. See [Section 3.1.4 on page 39](#) for details.
- 2 Disconnect and reconnect the switch’s power to begin a session. When you reconnect the switch’s power, you will see the initial screen.
- 3 When you see the message “Press any key to enter Debug Mode within 3 seconds . . .” press any key to enter debug mode.
- 4 Type `atlc` after the “Enter Debug Mode” message.
- 5 Wait for the “Starting XMODEM upload” message before activating XMODEM upload on your terminal.
- 6 After a configuration file upload, type `atgo` to restart the switch.

Figure 13 Resetting the Switch: Via the Console Port

```

Bootbase Version: V0.1 | 06/05/2006 18:30:17
RAM:Size = 32 Mbytes
DRAM POST: Testing: 32768K OK
DRAM Test SUCCESS !
FLASH: AMD 32M

ZyNOS Version: V3.60(AIH.0)C0 | 01/25/2007 11:33:20

Press any key to enter debug mode within 3 seconds.
.....
Enter Debug Mode
sysname> atlc
Starting XMODEM upload (CRC mode)....
CCCCCCCCCCCCCCCC
Total 393216 bytes received.
Erasing..
.....
OK
sysname> atgo

```

The switch is now reinitialized with a default configuration file including the default password of “1234”.

4.6 Logging Out of the Web Configurator

Click **Logout** in a screen to exit the web configurator. You have to log in with your password again after you log out. This is recommended after you finish a management session both for security reasons and so as you don’t lock out other switch administrators.

Figure 14 Web Configurator: Logout Screen

4.7 Help

The web configurator’s online help has descriptions of individual screens and some supplementary information.

Click the **Help** link from a web configurator screen to view an online help description of that screen.

System Status and Port Statistics

This chapter describes the system status (web configurator home page) and port details screens.

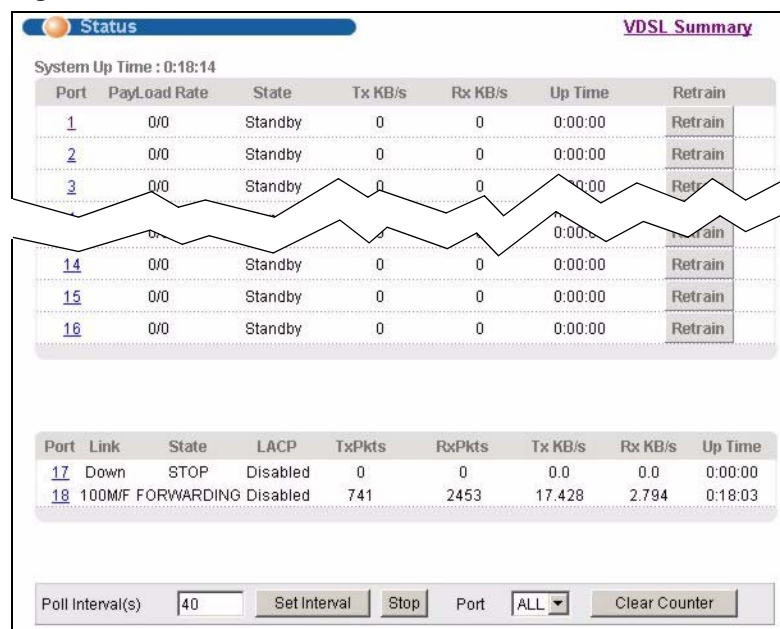
5.1 Overview

The home screen of the web configurator displays a port statistical summary with links to each port showing statistical details.

5.2 Port Status Summary

To view the port statistics, click **Status** in all web configurator screens to display the **Status** screen as shown next.

Figure 15 Status



The following table describes the labels in this screen.

Table 6 Status

LABEL	DESCRIPTION
System up Time	This field shows how long the system has been running since the last time it was started.
The following fields are related to the VDSL ports.	
Port	This identifies the VDSL port. Click a port number to display the VDSL Port Details screen.
PayLoad Rate	This field displays the upstream and downstream payload rates.
State	This field shows whether the port is connected (Showtime), not enabled (Idle) or is negotiating a connection (Training).
Tx KB/s	This field shows the number of kilobytes per second transmitted on this port.
Rx KB/s	This field shows the number of kilobytes per second received on this port.
Up Time	This field shows the total amount of time in hours, minutes and seconds the port has been up.
Retrain	Click Retrain to re-establish the line connection.
The following fields are related to the Ethernet ports.	
Port	This identifies the port. Click a port number to display the Port Details screen.
Link	This field displays the speed (10M for 10Mbps, 100M for 100Mbps or 1000M for 1000Mbps) and the duplex (F for full duplex or H for half duplex).
State	This field displays the STP state of the port. See the Spanning Tree Protocol chapter for details on STP port states.
LACP	This fields displays whether the Link Aggregation Control Protocol (LACP) has been enabled on the port.
TxPkts	This field shows the number of transmitted frames on this port.
RxPkts	This field shows the number of received frames on this port.
Errors	This field shows the number of received errors on this port.
Tx KB/s	This field shows the number of kilobytes per second transmitted on this port.
Rx KB/s	This field shows the number of kilobytes per second received on this port.
Up Time	This field shows the total amount of time in hours, minutes and seconds the port has been up.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking Set Interval .
Stop	Click Stop to halt system statistics polling.
Clear Counter	Select ALL in the Port field and then click Clear Counter to erase the recorded statistical information for all ports. Otherwise, select a port from the Port drop-down list box and then click Clear Counter to erase the recorded statistical information for that port.

5.2.1 VDSL Summary

To view VDSL statistics, click **VDSL Summary** in the **Status** screen.

Figure 16 Status: VDSL Summary

VDSL Summary								
Line NO	Name	State	Line Rate		PayLoad Rate		SNR Margin	
			Up	Down	Up	Down	Up	Down
1	port01	Standby	NA	NA	NA	NA	NA	NA
2	port02	Standby	NA	NA	NA	NA	NA	NA
3	port03	Standby	NA	NA	NA	NA	NA	NA
4	port04	Standby	NA	NA	NA	NA	NA	NA
5	port05	Standby	NA	NA	NA	NA	NA	NA
6	port06	Standby	NA	NA	NA	NA	NA	NA
7	port07	Standby	NA	NA	NA	NA	NA	NA
8	port08	Standby	NA	NA	NA	NA	NA	NA
9	port09	Standby	NA	NA	NA	NA	NA	NA
10	port10	Standby	NA	NA	NA	NA	NA	NA
11	port11	Standby	NA	NA	NA	NA	NA	NA
12	port12	Standby	NA	NA	NA	NA	NA	NA
13	port13	Standby	NA	NA	NA	NA	NA	NA
14	port14	Standby	NA	NA	NA	NA	NA	NA
15	port15	Standby	NA	NA	NA	NA	NA	NA
16	port16	Standby	NA	NA	NA	NA	NA	NA

5.2.2 VDSL Port Details

Click a number in the **Port** column in the **Status** screen to display individual port statistics. Use this screen to check status and detailed performance data about an individual port on the switch.

Figure 17 Status: VDSL Port Details

VDSL Port Details				Status
Port Info	Number	Port 1		
	Name	port01		
	Link Type	VDSL		
	State	Training		
	Up Time	0:00:00		
	Remote LAN Link 1	-----		
	Remote LAN Link 2	-----		
	Remote LAN Link 3	-----		
	Remote LAN Link 4	-----		
VDSL status	Items	Up Stream	Down Stream	
	Line Rate	0.000Mbps	0.000Mbps	
	Payload Rate	0.000Mbps	0.000Mbps	
	SNR Margin	0.0dB	0.0dB	
	Interleave Delay	0.0ms	0.0ms	
	Transmit Power	-----	0.0dBm	
	Attenuation	0.0dB	0.0dB	
	CRC Error	0	0	
	RS Correct	0	0	
	RS Uncorrect	0	0	
	ES	0	0	
	SES	0	0	
TX Packet	Tx Packets	1		
	Multicast	0		

TX Packet	TX Packets	1
	Multicast	0
	Broadcast	1
	Pause	0
RX Packet	RX Packets	0
	Multicast	0
	Broadcast	0
	Pause	0
	Control	0
TX Collision	Single	0
	Multiple	0
	Excessive	0
	Late	0
Error Packet	RX CRC	0
	Length	0
	Runt	0
Distribution	64	1
	65 to 127	0
	128 to 255	0
	256 to 511	0
	512 to 1023	0
	1024 to 1518	0
	Giant	0

VDSL Performance	Items	Vtuc	Vtur
	LOS	0	0
	LOF	0	0
	BMIN	0	0
	BERR	0	0
	Curr. 15 Min Time Elapsed	630	630
	LOS(15Min)	0	0
	LOF(15Min)	0	0
	BMIN(15Min)	0	0
	BERR(15Min)	0	0
	Curr. 1 Day Time Elapsed	2430	2430
	LOS(1Day)	0	0
	LOF(1Day)	0	0
	BMIN(1Day)	0	0
	BERR(1Day)	0	0

Poll Interval(s)

40

Set Interval

Stop

The following table describes the labels in this screen.

Table 7 Status: VDSL Port Details

LABEL	DESCRIPTION
Port Info	
Number	This field displays the port number.
Name	This field displays the descriptive name of a port.
Link Type	This field displays the type of the port.
State	This field displays the status of the port (Training , Idle or Showtime).
Up Time	This field shows the total amount of time the line has been up.
Remote LAN Link 1 .. 4	This field displays the status of the link to the remote CPE device.
VDSL Status	
Line Rate	This field displays the upstream/downstream transmission rate.

Table 7 Status: VDSL Port Details (continued)

LABEL	DESCRIPTION
Payload Rate	This field displays the upstream/downstream payload rate.
SNR Margin	This field displays the upstream/downstream SNR margin.
Interleave Delay	This field displays the upstream/downstream interleave delay.
Transmit Power	This field displays the upstream/downstream transmission power of the line.
Attenuation	This field displays the upstream/downstream attenuation.
CRC Error	This field displays the number of CRC (Cyclical Redundancy Check) error packet.
RS Correct	This field displays the number of Reed-Solomon (RS) correct packets.
RS Uncorrect	This field displays the number of Reed-Solomon (RS) uncorrect packets.
ES	This displays port endpoint errored seconds (ESs).
SES	This displays port endpoint severely errored seconds (SESS).
Tx Packet	
Tx Packets	This field displays the number of packets transmitted.
Multicast	This field shows the number of good multicast packets transmitted.
Broadcast	This field shows the number of good broadcast packets transmitted.
Pause	This field shows the number of 802.3x Pause frames transmitted.
Rx Packet	
Rx Packets	This field displays the number of packets received.
Multicast	This field shows the number of good multicast packets received.
Broadcast	This field shows the number of good broadcast packets received.
Pause	This field shows the number of 802.3x Pause frames received.
Control	This field shows the number of control received (including those with CRC error) but it does not include the 802.3x Pause frames.
Tx Collision	
Single	This field shows the number of packets with 1 collision detected.
Multiple	This field shows the number of packets with 2 to 15 collisions detected.
Excessive	This field shows the number of packets with in excess of 15 collisions detected.
Late	A late collision is counted when a device detects a collision after it has sent the 512th bit of its frame. This field shows the number of times such a collision is detected.
Error Packet	
Rx CRC	This field shows the number of frames with CRC (Cyclic Redundant Check) error(s).
Length	This field shows the number of frames with a length that was out of range.
Runt	This field shows the number of frames received that were too short (shorter than 64 octets), including the ones with CRC errors.
Distribution	
64	This field shows the number of packets (including bad packets) transmitted that were 64 octets in length.
65-127	This field shows the number of packets (including bad packets) transmitted that were between 65 and 127 octets in length.

Table 7 Status: VDSL Port Details (continued)

LABEL	DESCRIPTION
128-255	This field shows the number of packets (including bad packets) transmitted that were between 128 and 255 octets in length.
256-511	This field shows the number of packets (including bad packets) transmitted that were between 256 and 511 octets in length.
512-1023	This field shows the number of packets (including bad packets) transmitted that were between 512 and 1023 octets in length.
1024-1518	This field shows the number of packets (including bad packets) transmitted that were between 1024 and 1518 octets in length.
Giant	This field shows the number of packets (including bad packets) transmitted that were longer than 1518 octets in length.
VDSL Performance	
LOS	This field displays the number of Loss of Signal (LOS) failures.
LOF	This field displays the number of Loss of Framing (LOF) failures.
BMIN	If the actual SNR falls below the minimum SNR, the DSL connection will be dropped and re-initialized. This field displays how many times the connection has been dropped due to the average SNR' falling below the specified minimum SNR.
BERR	This field displays how many times the connection has been dropped due to the CRC errors' being increasing for more than 30 consecutive seconds.
Curr. 15 Min. Time Elapsed	This field displays the total number of errors detected within the last 15-minute (900 second) time segment. The counter resets to zero after the time segment elapses.
LOS (15Min)	This field displays the number of Loss of Signal (LOS) failures within the last 15 minute (900 second) time segment. The counter resets to zero after the time segment elapses.
LOF (15Min)	This field displays the number of Loss of Framing (LOF) failures within the last 15 minute (900 second) time segment. The counter resets to zero after the time segment elapses.
BMIN (15Min)	This field displays how many times the connection has been dropped due to the average SNR' falling below the specified minimum SNR within the last 15 minute (900 second) time segment. The counter resets to zero after the time segment elapses.
BERR (15Min)	This field displays how many times the connection has been dropped due to the CRC errors' being increasing for more than 30 consecutive seconds within the last 15 minute (900 second) time segment. The counter resets to zero after the time segment elapses.
Curr. 1 Day Time Elapsed	This field displays the total number of errors detected within the last 1-day time segment. The counter resets to zero after the time segment elapses.
LOS (1Day)	This field displays the number of Loss of Signal (LOS) failures within the last 1-day time segment. The counter resets to zero after the time segment elapses.
LOF (1 Day)	This field displays the number of Loss of Framing (LOF) failures within the last 1-day period. The counter resets to zero after the time segment elapses.
BMIN (1 Day)	This field displays how many times the connection has been dropped due to the average SNR's falling below the specified minimum SNR within the last 1-day period. The counter resets to zero after the time segment elapses.
BERR (1 Day)	This field displays how many times the connection has been dropped due to the CRC errors being increasing for more than 30 consecutive seconds within the last 1-day period. The counter resets to zero after the time segment elapses.

Table 7 Status: VDSL Port Details (continued)

LABEL	DESCRIPTION
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking Set Interval .
Stop	Click Stop to stop port statistic polling.

5.2.3 Ethernet Port Details

Click a number in the **Port** column in the **Status** screen to display the Ethernet port statistics. Use this screen to check status and detailed performance data about an Ethernet port on the switch.

Figure 18 Status: Port Details

Port Details			Status
Port Info	Port NO.	17	
	Link	1000M/F	
	Status	FORWARDING	
	LACP	Disabled	
	TxPkts	105	
	RxPkts	88	
	Errors	0	
	Tx KBs/s	0.0	
	Rx KBs/s	0.0	
	Up Time	0:00:42	
TX Packet	TX Packets	105	
	Multicast	0	
	Broadcast	3	
	Pause	0	
RX Packet	RX Packets	88	
	Multicast	0	
	Broadcast	0	
	Pause	0	
	Control	0	
TX Collision	Single	0	
	Multiple	0	
	Excessive	0	
	Late	0	
Error Packet	RX CRC	0	
	Length	0	
	Runt	0	
Distribution	64	89	
	65 to 127	10	
	128 to 255	6	
	256 to 511	35	
	512 to 1023	5	
	1024 to 1518	48	
	Giant	0	
Poll Interval(s) 40			
Set Interval			
Stop			

The following table describes the labels in this screen.

Table 8 Status: Port Details

LABEL	DESCRIPTION
Port Info	
Link	This field displays the speed (either 10M for 10Mbps, 100M for 100Mbps or 1000M for 1000Mbps) and the duplex (F for full duplex or H for half duplex). It also shows the cable type (Copper or Fiber) for the combo ports.
Status	If STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port (see Section 10.1.3 on page 102 for more information). If STP is disabled, this field displays FORWARDING if the link is up, otherwise, it displays STOP .
LACP	This field shows if LACP is enabled on this port or not.
TxPkts	This field shows the number of transmitted frames on this port
RxPkts	This field shows the number of received frames on this port
Errors	This field shows the number of received errors on this port.
Tx KB/s	This field shows the number kilobytes per second transmitted on this port.
Rx KB/s	This field shows the number of kilobytes per second received on this port.
Up Time	This field shows the total amount of time the connection has been up.
Tx Packet	
The following fields display detailed information about packets transmitted.	
TX Packets	This field shows the number of good packets (unicast, multicast and broadcast) transmitted.
Multicast	This field shows the number of good multicast packets transmitted.
Broadcast	This field shows the number of good broadcast packets transmitted.
Pause	This field shows the number of 802.3x Pause packets transmitted.
Rx Packet	
The following fields display detailed information about packets received.	
RX Packets	This field shows the number of good packets (unicast, multicast and broadcast) received.
Multicast	This field shows the number of good multicast packets received.
Broadcast	This field shows the number of good broadcast packets received.
Pause	This field shows the number of 802.3x Pause packets received.
Control	This field shows the number of control packets received (including those with CRC error) but it does not include the 802.3x Pause packets.
TX Collision	
The following fields display information on collisions while transmitting.	
Single	This is a count of successfully transmitted packets for which transmission is inhibited by exactly one collision.
Multiple	This is a count of successfully transmitted packets for which transmission was inhibited by more than one collision.
Excessive	This is a count of packets for which transmission failed due to excessive collisions. Excessive collision is defined as the number of maximum collisions before the retransmission count is reset.
Late	This is the number of times a late collision is detected, that is, after 512 bits of the packets have already been transmitted.

Table 8 Status: Port Details (continued)

LABEL	DESCRIPTION
Error Packet	The following fields display detailed information about packets received that were in error.
RX CRC	This field shows the number of packets received with CRC (Cyclic Redundant Check) error(s).
Length	This field shows the number of packets received with a length that was out of range.
Runt	This field shows the number of packets received that were too short (shorter than 64 octets), including the ones with CRC errors.
Distribution	
64	This field shows the number of packets (including bad packets) received that were 64 octets in length.
65-127	This field shows the number of packets (including bad packets) received that were between 65 and 127 octets in length.
128-255	This field shows the number of packets (including bad packets) received that were between 128 and 255 octets in length.
256-511	This field shows the number of packets (including bad packets) received that were between 256 and 511 octets in length.
512-1023	This field shows the number of packets (including bad packets) received that were between 512 and 1023 octets in length.
1024-1518	This field shows the number of packets (including bad packets) received that were between 1024 and 1518 octets in length.
Giant	This field shows the number of packets dropped because they were bigger than the maximum frame size.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking Set Interval .
Stop	Click Stop to stop port statistic polling.

Basic Setting

This chapter describes how to configure the **System Info**, **General Setup**, **Switch Setup**, **IP Setup** and **Port Setup** screens.

6.1 Overview

The **System Info** screen displays general switch information (such as firmware version number) and hardware polling information (such as fan speeds). The **General Setup** screen allows you to configure general switch identification information. The **General Setup** screen also allows you to set the system time manually or get the current time and date from an external server when you turn on your switch. The real time is then displayed in the switch logs. The **Switch Setup** screen allows you to set up and configure global switch features. The **IP Setup** screen allows you to configure a switch IP address, subnet mask(s) and DNS (domain name server) for management purposes.

6.2 System Information

In the navigation panel, click **Basic Setting** and **System Info** to display the screen as shown. You can check the firmware version number and the device MAC address, and monitor the switch temperature, fan speeds and voltage in this screen.

Figure 19 System Info

System Info

System Name	VES-1616F-35
OS F/W Version	V3.60(AIH.0)C0 01/25/2007
Modem Code F/W Version	1.0.5r11IK004010
Ethernet Address	00:13:49:00:00:02

Hardware Monitor

Temperature Unit:

Temperature (C)	Current	MAX	MIN	Threshold	Status
IFE8	50.0	50.0	29.0	81.0	Normal
Switch	36.0	37.0	23.0	73.0	Normal
ADT7463	35.0	36.0	25.0	88.0	Normal

FAN Speed (RPM)	Current	MAX	MIN	Threshold	Status
FAN1	3454	6101	3358	1000	Normal
FAN2	3602	6308	3422	1000	Normal
FAN3	3483	6129	3327	1000	Normal
FAN4	3400	7049	3199	1000	Normal

Voltage (V)	Current	MAX	MIN	Threshold	Status
2.5VIN	2.506	2.506	2.506	+/- 6%	Normal
1.2VIN	1.201	1.201	1.189	+/- 6%	Normal
3.3VIN	3.320	3.320	3.320	+/- 6%	Normal
12.0VIN	12.031	12.031	12.031	+/- 6%	Normal

Poll Interval(s):

The following table describes the labels in this screen.

Table 9 System Info

LABEL	DESCRIPTION
System Name	This field displays the descriptive name of the switch for identification purposes.
OS F/W Version	This field displays the version number of the switch 's current firmware including the date created.
Modem Code F/W Version	This field displays the version number of the switch 's current VDSL modem code version.
Ethernet Address	This field refers to the Ethernet MAC (Media Access Control) address of the switch.
Hardware Monitor	
Temperature Unit	The switch has temperature sensors that are capable of detecting and reporting if the temperature rises above the threshold. You may choose the temperature unit (Centigrade or Fahrenheit) in this field.
Temperature	IFE8 , Switch and ADT7463 refer to the location of the temperature sensors on the circuit board.
Current	This shows the current temperature in degrees centigrade at this sensor.
MAX	This field displays the maximum temperature measured at this sensor.
MIN	This field displays the minimum temperature measured at this sensor.
Threshold	This field displays the upper temperature limit at this sensor.
Status	This field displays Normal for temperatures below the threshold and Error for those above. If Error displays, check that the fans are working and make sure that you do not block ventilation holes on the switch.
Fan Speed (RPM)	A properly functioning fan is an essential component (along with a sufficiently ventilated, cool operating environment) in order for the device to stay within the temperature threshold. Each fan has a sensor that is capable of detecting and reporting if the fan speed falls below the threshold shown.

Table 9 System Info (continued)

LABEL	DESCRIPTION
Current	This field displays this fan's current speed in Revolutions Per Minute (RPM).
MAX	This field displays this fan's maximum speed measured in Revolutions Per Minute (RPM).
MIN	This field displays this fan's minimum speed measured in Revolutions Per Minute (RPM).
Threshold	This field displays the minimum speed at which a normal fan should work.
Status	Normal indicates that this fan is functioning above the minimum speed. Error indicates that this fan is functioning below the minimum speed. If Error displays, it is recommended that the fan(s) on the switch be replaced by a qualified technician.
Voltage (V)	The power supply for each voltage has a sensor that is capable of detecting and reporting if the voltage falls out of the tolerance range.
Current	This is the current voltage reading.
MAX	This field displays the maximum voltage measured at this point.
MIN	This field displays the minimum voltage measured at this point.
Threshold	This field displays the percentage tolerance of the voltage with which the switch still works.
Status	Normal indicates that the voltage is within an acceptable operating range at this point; otherwise Error is displayed. If Error displays, an electronic component might be defective. Have the switch serviced by a qualified technician.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking Set Interval .
Stop	Click Stop to stop port statistic polling.

6.3 General Setup

Click **Basic Setting** and **General Setup** in the navigation panel to display the screen as shown. Use this screen to configure the system name, the system time and date and specify the login authentication database priority.

Figure 20 General Setup

General Setup

System Name

Location

Contact Person's Name

Login Precedence

Use Time Server when Bootup

Time Server IP Address

Current Time : :

New Time (hh:mm:ss) : :

Current Date - -

New Date (yyyy-mm-dd) - -

Time Zone

It will take 60 seconds if time server is unreachable.

The following table describes the labels in this screen.

Table 10 General Setup

LABEL	DESCRIPTION
System Name	Choose a descriptive name for identification purposes. This name consists of up to 32 printable characters; spaces are not allowed.
Location	Enter the geographic location (up to 30 characters) of your switch.
Contact Person's Name	Enter the name (up to 30 characters) of the person in charge of this switch.
Login Precedence	<p>Use this drop-down list box to select which database the switch should use (first) to authenticate an administrator (user for switch management).</p> <p>Configure the local user accounts in the Access Control Logins screen. The RADIUS is an external server. Before you specify the priority, make sure you have set up the corresponding database correctly first.</p> <p>Select Local Only to have the switch just check the local user accounts configured in the Access Control Logins screen.</p> <p>Select Local then RADIUS to have the switch check the local user accounts configured in the Access Control Logins screen. If the user name is not found, the switch then checks the user database on the specified RADIUS server. You need to configure Port Authentication RADIUS first.</p> <p>Select RADIUS Only to have the switch just check the user database on the specified RADIUS server for a login username and password.</p>

Table 10 General Setup (continued)

LABEL	DESCRIPTION
Use Time Server when Bootup	<p>Enter the time service protocol that a timeserver sends when you turn on the switch. Not all time servers support all protocols, so you may have to use trial and error to find a protocol that works. The main differences between them are the time format.</p> <p>When you select the Daytime (RFC 867) format, the switch displays the day, month, year and time with no time zone adjustment. When you use this format it is recommended that you use a Daytime timeserver within your geographical time zone.</p> <p>Time (RFC-868) format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.</p> <p>NTP (RFC-1305) is similar to Time (RFC-868).</p> <p>None is the default value. Enter the time manually. Each time you turn on the switch, the time and date will be reset to 2000-1-1 0:0.</p>
Time Server IP Address	Enter the IP address of your timeserver. The switch searches for the timeserver for up to 60 seconds. If you select a timeserver that is unreachable, then this screen will appear locked for 60 seconds. Please wait.
Current Time	This field displays the time you open this menu (or refresh the menu).
New Time (hh:min:ss)	Enter the new time in hour, minute and second format. The new time then appears in the Current Time field after you click Apply .
Current Date	This field displays the date you open this menu.
New Date (yyyy-mm-dd)	Enter the new date in year, month and day format. The new date then appears in the Current Date field after you click Apply .
Time Zone	Select the time difference between UTC (Universal Time Coordinated), formerly known as GMT (Greenwich Mean Time) and your time zone from the drop-down list box.
Apply	Click Apply to save the settings.
Cancel	Click Cancel to reset the fields to your previous configuration.

6.4 Introduction to VLANs

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

In MTU (Multi-Tenant Unit) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN, thus a user will not see the printers and hard disks of another user in the same building.

VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.



VLAN is unidirectional; it only governs outgoing traffic.

See [Chapter 7 on page 87](#) for information on port-based and IEEE 802.1Q tagged VLANs.

6.5 Switch Setup Screen

Click **Basic Setting** and then **Switch Setup** in the navigation panel to display the screen as shown. The VLAN setup screens change depending on whether you choose **802.1Q** or **Port Based** in the **VLAN Type** field in this screen. Refer to the chapter on VLAN.

Figure 21 Switch Setup

The following table describes the labels in this screen.

Table 11 Switch Setup

LABEL	DESCRIPTION
VLAN Type	Choose 802.1Q or Port Based . The VLAN Setup screen changes depending on whether you choose 802.1Q VLAN type or Port Based VLAN type in this screen. See Chapter 7 on page 87 for more information.
Bridge Control Protocol Transparency	Select Active to allow the switch to handle bridging control protocols (STP for example). You also need to define how to treat a BPDU in the Port Setup screen.
MAC Address Learning	MAC address learning reduces outgoing traffic broadcasts. For MAC address learning to occur on a port, the port must be active.
Aging Time	Enter a time from 10 to 3000 seconds. This is how long all dynamically learned MAC addresses remain in the MAC address table before they age out (and must be relearned).

Table 11 Switch Setup (continued)

LABEL	DESCRIPTION
	GARP Timer: Switches join VLANs by making a declaration. A declaration is made by issuing a Join message using GARP. Declarations are withdrawn by issuing a Leave message. A Leave All message terminates all registrations. GARP timers set declaration timeout values. See the chapter on VLAN setup for more background information.
Join Timer	Join Timer sets the duration of the Join Period timer for GVRP in milliseconds. Each port has a Join Period timer. The allowed Join Time range is between 100 and 65535 milliseconds; the default is 200 milliseconds. See the chapter on VLAN setup for more background information.
Leave Timer	Leave Time sets the duration of the Leave Period timer for GVRP in milliseconds. Each port has a single Leave Period timer. Leave Time must be two times larger than Join Timer ; the default is 600 milliseconds.
Leave All Timer	Leave All Timer sets the duration of the Leave All Period timer for GVRP in milliseconds. Each port has a single Leave All Period timer. Leave All Timer must be larger than Leave Timer; the default is 1000 milliseconds.
<p>Priority Queue Assignment</p> <p>IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Frames without an explicit priority tag are given the default priority of the ingress port. Use the following fields to configure the priority level-to-physical queue mapping.</p> <p>The switch has eight physical queues that you can map to the 8 priority levels. On the switch, traffic assigned to higher index queues gets through faster while traffic in lower index queues is dropped if the network is congested.</p> <p>Priority Level (The following descriptions are based on the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).</p>	
Level 7	Typically used for network control traffic such as router configuration messages.
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Level 3	Typically used for "excellent effort" or better than best effort and would include important business traffic that can tolerate some delay.
Level 2	This is for "spare bandwidth".
Level 1	This is typically used for non-critical "background" traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Level 0	Typically used for best-effort traffic.
Apply	Click Apply to save the settings.
Cancel	Click Cancel to reset the fields to your previous configuration.

6.6 IP Setup

Use the **IP Setup** screen to configure the default gateway device, the management IP address and the default domain name server.

6.6.1 Management IP Address

The switch needs an IP address for it to be managed over the network. The factory default in-band IP address is 192.168.1.1 and out-of-band management IP is 192.168.0.1. The subnet mask specifies the network number portion of an IP address. The factory default subnet mask is 255.255.255.0.

You can configure up to 128 IP addresses which are used to access and manage the switch from the ports belonging to the pre-defined VLAN(s).



You must configure a VLAN first.

Figure 22 IP Setup

IP Setup

Domain Name Server: 0.0.0.0

Default Management: ☒ In-band ☐ Out-of-band

In-band Management IP Address

☐ DHCP Client

☒ Static IP Address

IP Address: 192.168.1.1

IP Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

VID: 1

Out-of-band Management IP Address

IP Address: 192.168.0.1

IP Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

Apply Cancel

In-band IP Addresses

IP Address	0.0.0.0
IP Subnet Mask	0.0.0.0
VID	
Default Gateway	0.0.0.0
Manageable	<input type="checkbox"/>

Add Cancel

Index	IP Address	IP Subnet Mask	VID	Default Gateway	Manageable	Delete

Delete Cancel

The following table describes the labels in this screen.

Table 12 IP Setup

LABEL	DESCRIPTION
Domain Name Server	Enter the IP address of the domain name server in dotted decimal notation, for example 192.168.1.20.
Default Management	<p>Select which traffic flow (In-Band or Out-of-band) the switch is to use to send packets with an unknown source or that originated from the switch itself (such as SNMP traps).</p> <p>Select Out-of-band to have the switch send the packets to the out-of-band management port. This means that device(s) connected to the other port(s) do not receive these packets.</p> <p>Select In-Band to have the switch send the packets to all ports except the out-of-band management port. This means that device(s) connected to out-of-band management port do not receive these packets.</p>
In-band Management IP Address	
DHCP Client	Select this option if you have a DHCP server that can assign the switch an IP address and subnet mask, a default gateway IP address and a domain name server IP address.
Static IP Address	Select this option if you don't have a DHCP server or if you wish to assign static IP address information to the switch. You need to fill in the following fields when you select this option.
IP Address	Enter the IP address of your switch in dotted decimal notation for example 192.168.1.1.
IP Subnet Mask	Enter the IP subnet mask of your switch in dotted decimal notation for example 255.255.255.0.
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254
VID	Enter the VLAN identification number associated with the switch IP address. This is the VLAN ID of the CPU and is used for management only. The default is "1". All ports, by default, are fixed members of this "management VLAN" in order to manage the device from any port. If a port is not a member of this VLAN, then users on that port cannot access the device. To access the switch make sure the port that you are connected to is a member of Management VLAN.
Out-of-band Management IP Address	
IP Address	Enter the IP address of your switch in dotted decimal notation for example 192.168.0.1.
IP Subnet Mask	Enter the IP subnet mask of your switch in dotted decimal notation for example 255.255.255.0.
Apply	Click Apply to save the settings.
Cancel	Click Cancel to reset the fields to your previous configuration.
In-band IP Addresses	
You can create up to 128 IP addresses, which are used to access and manage the switch from the ports belonging to the pre-defined VLAN(s). You must configure a VLAN first.	
IP Address	Enter the IP address for managing the switch by the members of the VLAN specified in the VID field below.
IP Subnet Mask	Enter the IP subnet mask in dotted decimal notation.
VID	Type the VLAN group identification number.
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation.

Table 12 IP Setup (continued)

LABEL	DESCRIPTION
Manageable	Select this option to allow device management using this IP address setting. Clear this option to set the switch to block management access using this IP address.
Add	Click Add to save the new rule to the switch. It then displays in the summary table at the bottom of the screen.
Cancel	Click Cancel to reset the fields to your previous configuration.
Index	This field displays the index number of the rule. Click an index number to edit the rule.
IP Address	This field displays the IP address.
IP Subnet Mask	This field displays the subnet mask.
VID	This field displays the ID number of the VLAN group.
Default Gateway	This field displays the IP address of the default gateway.
Manageable	This field displays whether device management on this IP address is allowed.
Delete	Check the rule(s) that you want to remove in the Delete column, then click the Delete button.
Cancel	Click Cancel to clear the selected checkboxes in the Delete column.

6.7 Port Setup

Click **Basic Setting** and then **Port Setup** in the navigation panel to display the configuration screen. Use this screen to configure general VDSL and Ethernet port settings.

Figure 23 Port Setup

Port	Active	Name	Type	Profile	PSD Profile	Alarm Profile	Flow Control	802.1p Priority	BPDU Control
1	<input checked="" type="checkbox"/>	port01	VDSL	DEFVAL	DEFVAL	DEFVAL	<input checked="" type="checkbox"/>	0	Peer
2	<input checked="" type="checkbox"/>	port02	VDSL	DEFVAL	DEFVAL	DEFVAL	<input checked="" type="checkbox"/>	0	Peer
3	<input checked="" type="checkbox"/>	port03	VDSL	DEFVAL	DEFVAL	DEFVAL	<input checked="" type="checkbox"/>	0	Peer
4	<input checked="" type="checkbox"/>	port04	VDSL	DEFVAL	DEFVAL	DEFVAL	<input checked="" type="checkbox"/>	0	Peer
5	<input checked="" type="checkbox"/>	port05	VDSL	DEFVAL	DEFVAL	DEFVAL	<input checked="" type="checkbox"/>	0	Peer
6	<input checked="" type="checkbox"/>	port06	VDSL	DEFVAL	DEFVAL	DEFVAL	<input checked="" type="checkbox"/>	0	Peer
7	<input checked="" type="checkbox"/>	port07	VDSL	DEFVAL	DEFVAL	DEFVAL	<input checked="" type="checkbox"/>	0	Peer
8	<input checked="" type="checkbox"/>	port08	VDSL	DEFVAL	DEFVAL	DEFVAL	<input checked="" type="checkbox"/>	0	Peer
9	<input checked="" type="checkbox"/>	port09	VDSL	DEFVAL	DEFVAL	DEFVAL	<input checked="" type="checkbox"/>	0	Peer
10	<input checked="" type="checkbox"/>	port10	VDSL	DEFVAL	DEFVAL	DEFVAL	<input checked="" type="checkbox"/>	0	Peer
11	<input checked="" type="checkbox"/>	port11	VDSL	DEFVAL	DEFVAL	DEFVAL	<input checked="" type="checkbox"/>	0	Peer
12	<input checked="" type="checkbox"/>	port12	VDSL	DEFVAL	DEFVAL	DEFVAL	<input checked="" type="checkbox"/>	0	Peer
13	<input checked="" type="checkbox"/>	port13	VDSL	DEFVAL	DEFVAL	DEFVAL	<input checked="" type="checkbox"/>	0	Peer
14	<input checked="" type="checkbox"/>	port14	VDSL	DEFVAL	DEFVAL	DEFVAL	<input checked="" type="checkbox"/>	0	Peer
15	<input checked="" type="checkbox"/>	port15	VDSL	DEFVAL	DEFVAL	DEFVAL	<input checked="" type="checkbox"/>	0	Peer
16	<input checked="" type="checkbox"/>	port16	VDSL	DEFVAL	DEFVAL	DEFVAL	<input checked="" type="checkbox"/>	0	Peer

Port	Active	Name	Type	Speed / Duplex	Flow Control	802.1p Priority	BPDU Control
17	<input checked="" type="checkbox"/>	port17	10/100/1000M	Auto	<input checked="" type="checkbox"/>	0	Peer
18	<input checked="" type="checkbox"/>	port18	10/100/1000M	Auto	<input checked="" type="checkbox"/>	0	Peer

Apply Cancel

The following table describes the labels in this screen.

Table 13 Port Setup

LABEL	DESCRIPTION
Ports 1 .. 16	
Port	This is the port index number.
Active	Select this check box to enable a port. The factory default for all ports is enabled. A port must be enabled for data transmission to occur.
Name	Enter a descriptive name that identifies this port. You can enter up to 64 alpha-numerical characters. Note: Due to space limitation, the port name may be truncated in some web configurator screens.
Type	This field displays VDSL for the VDSL ports.
Profile	Select a VDSL line profile from the drop-down list box. This field displays the profile names you configure in the VDSL Profile Setup screen. Refer to Section 6.9 on page 77 for more information.
PSD Profile	Select a VDSL PSD profile from the drop-down list box. This field displays the profile names you configure in the VDSL PSD Profile Setup screen. Refer to Section 6.11 on page 82 for more information.
Alarm Profile	Select a VDSL alarm profile from the drop-down list box. This field displays the alarm profile names you configure in the VDSL Alarm Profile Setup screen. Refer to Section 6.10 on page 80 for more information.

Table 13 Port Setup (continued)

LABEL	DESCRIPTION
Flow Control	<p>A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. Flow Control is used to regulate transmission of signals to match the bandwidth of the receiving port.</p> <p>The switch uses IEEE 802.3x flow control in full duplex mode and back pressure flow control in half duplex mode.</p> <p>IEEE 802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill.</p> <p>Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later. Select Flow Control to enable it.</p>
802.1P Priority	<p>This priority value is added to incoming frames without a (802.1p) priority queue tag. See Priority Queue Assignment in Table 11 on page 68 for more information.</p>
BPDU Control	<p>Configure the way to treat BPDUs received on this port. You must activate bridging control protocol transparency in the Switch Setup screen first.</p> <p>Select Peer to process any BPDU (Bridge Protocol Data Units) received on this port.</p> <p>Select Tunnel to forward BPDUs received on this port.</p> <p>Select Discard to drop any BPDU received on this port.</p> <p>Select Network to process a BPDU with no VLAN tag and forward a tagged BPDU.</p>
Ports 17, 18	
Port	This is the port index number.
Active	Select this check box to enable a port. The factory default for all ports is enabled. A port must be enabled for data transmission to occur.
Name	<p>Enter a descriptive name that identifies this port. You can enter up to 64 alpha-numerical characters.</p> <p>Note: Due to space limitation, the port name may be truncated in some web configurator screens.</p>
Type	This field displays 10/100/1000M for the Gigabit/ mini GBIC combo ports or 1000M for the mini GBIC ports.
Speed/Duplex	<p>Select the speed and the duplex mode of the connection on this port. Choices are Auto, 10M/Half Duplex, 10M/Full Duplex, 100M/Half Duplex, 100M/Full Duplex and 1000M/Full Duplex.</p> <p>Selecting Auto (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.</p>

Table 13 Port Setup (continued)

LABEL	DESCRIPTION
Flow Control	<p>A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. Flow Control is used to regulate transmission of signals to match the bandwidth of the receiving port.</p> <p>The switch uses IEEE802.3x flow control in full duplex mode and back pressure flow control in half duplex mode.</p> <p>IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill.</p> <p>Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later. Select Flow Control to enable it.</p>
802.1P Priority	<p>This priority value is added to incoming frames without a (802.1p) priority queue tag. See Priority Queue Assignment in Table 11 on page 68 for more information.</p>
BPDU Control	<p>Configure the way to treat BPDUs received on this port. You must activate bridging control protocol transparency in the Switch Setup screen first.</p> <p>Select Peer to process any BPDU (Bridge Protocol Data Units) received on this port.</p> <p>Select Tunnel to forward BPDUs received on this port.</p> <p>Select Discard to drop any BPDU received on this port.</p> <p>Select Network to process a BPDU with no VLAN tag and forward a tagged BPDU.</p>
Apply	Click Apply to save the settings.
Cancel	Click Cancel to reset the fields to your previous configuration.

6.8 VDSL Parameters

The following sections describe the VDSL parameters you configure in the following screens:

- VDSL Profile Setup (see [Section 6.9 on page 77](#)).
- VDSL Alarm Profile Setup (see [Section 6.10 on page 80](#)).
- VDSL PSD Profile Setup (see [Section 6.11 on page 82](#)).

6.8.1 Frequency Band Plan

Each VDSL mode operates in a different frequency band allocation, resulting in different upstream and downstream speeds. Your VES switch automatically changes the band plan based on the loop condition and loop length.

All of the band plans include an optional band. Use the optional band for upstream transmission which is to be negotiated during line initiation.

6.8.2 Configured Versus Actual Rate

You configure the maximum rate of an individual VDSL port by modifying its profile (see the **VDSL Profile Setup** screen) or assigning the port to a different profile (see the **Port Setup** screen). However, the actual rate varies depending on factor such as transmission range and interference.

6.8.3 PSD

PSD (Power Spectral Density) defines the distribution of a VDSL line's power in the frequency domain. A PSD mask specifies the maximum allowable PSD for a line.

6.8.4 UPBO

In a network with varying telephone wiring lengths, the PSD on each line is different. This causes crosstalk between the lines. Enable UPBO (Upstream Power Back Off) to allow the switch to adjust the transmit PSD of all lines based on a reference line length so that the PSD at the receiving end is the same.

6.8.5 Latency Modes

There are two latency modes: interleave and fast.

- Interleave

Interleave delay is the wait (in milliseconds) that determines the size of a single block of data to be interleaved (assembled) and then transmitted. Interleave delay is used when transmission error correction (Reed- Solomon) is necessary due to a less-than-ideal telephone line. The bigger the delay, the bigger the data block size, allowing better error correction to be performed.

Reed-Solomon codes are block-based error correcting codes with a wide range of applications. The Reed-Solomon encoder takes a block of digital data and adds extra "redundant" bits. The Reed-Solomon decoder processes each block and attempts to correct errors and recover the original data.

- Fast

Fast mode means no interleaving takes place and transmission is faster (a "fast channel"). This would be suitable if you have a good line where little error correction is necessary.

6.8.6 Rate Adaption

Rate adaption is the ability of a device to adjust from the configured transmission rate to the attainable transmission rate automatically depending on the line quality. The VDSL transmission rate then stays at the new rate or adjusts if line quality improves or deteriorates.

The switch determines line quality using the Signal-to-Noise Ratio (SNR). SNR is the ratio of the amplitude of the actual signal to the amplitude of noise signals at a given point in time. A low SNR indicates poor line quality.

If you disable transmission rate adjustment and the attainable speeds cannot match configured speeds, then the VDSL link may go down or link communications may be sporadic due to line errors and consequent retransmissions

Enable the switch to adjust to a new lower rate when the line quality deteriorates until the connection is broken. The switch will first disconnect and then re-establish the line connection to maintain connectivity. However, the new line rate might be lower or higher than the configured line rate.

6.8.7 RFI (Radio Frequency Interference)

RFI is induced noise on the lines by surrounding radio frequency electromagnetic radiation from sources such as AM and HAM radio stations. Since the VDSL uses a much larger frequency range that overlaps with other radio frequency systems, signals from VDSL lines and other radio systems interfere with each other. To avoid performance degradation due to RFI, set the switch to not transmit VDSL signals in the RFI band.

6.8.8 VDSL Profiles

A profile is a table that contains a list of pre-configured VDSL line settings or VDSL alarm threshold settings. Each VDSL port has one (and only one) line and alarm profile assigned to it at any given time.

Profiles allow you to configure VDSL ports efficiently. You can configure all of the VDSL ports with the same profile, thus removing the need to configure the VDSL ports one-by-one. You can also change an individual VDSL port by assigning it a different profile.

For example, you could set up different profiles for different kinds of accounts (for example, economy, standard and premium). Assign the appropriate profile to a VDSL port and it takes care of a large part of the port's configuration.

6.9 VDSL Profile Setup

The line profile defines VDSL parameters such as the payload rates, the upstream/downstream signal noise margins and impulse noise protection. You can configure multiple profiles, including profiles for troubleshooting.

To configure or view VDSL profiles, click **Basic Setting** and **VDSL Profile Setup** to display the screen as shown next.

Figure 24 VDSL Profile Setup

VDSL Profile Setup

Name: DEFVAL

DownStream

Slow Channel Payload Rate: MAX 104960 MIN 64

Fast Channel Payload Rate: MAX 104960 MIN 64

Rate Adaptive: ☒ Manual ☐ AdaptAtInit

Max SNR: 31.75dB

Target SNR: 6dB

Min SNR: 0dB

MaxInterleave Delay: 2 ms

Max Aggregate Power: 14.5 dbm

Rate Ratio: 0 %

Impulse Noise Protection: 0 ms

FEC Redundancy: 0 %

Template PSD Mask: ☐ Mask1 ☒ Mask2

PBO Control: Disable

PBO Level: 0dB

Band Plan: BandPlan998

Band Plan FX: 12000 kHz

Applicable Standard: ☒ ANSI ☒ ETSI ☐ ITU ☐ other

Deployment Scenario: ☐ FTTCab ☒ FTTEEx ☐ other

Compatible Mode: ☐ None ☐ 640kHz ☐ 1100kHz ☒ 2200kHz

Ham Band Plan

	start	stop
<input type="checkbox"/> CustomNotch1	0 kHz	0 kHz
<input type="checkbox"/> CustomNotch2	0 kHz	0 kHz
<input type="checkbox"/> Amateur Radio	1810kHz	2000kHz
<input type="checkbox"/> Amateur Radio	3500kHz	3800kHz(ETSI); 4000kHz(ANSI)
<input type="checkbox"/> Amateur Radio	7000kHz	7100kHz(ETSI); 7300kHz(ANSI)
<input type="checkbox"/> Amateur Radio	10100kHz	10150kHz
<input type="checkbox"/> Amateur Radio	14000kHz	14350kHz
<input checked="" type="checkbox"/> Amateur Radio	18068kHz	18168kHz
<input checked="" type="checkbox"/> Amateur Radio	21000kHz	21450kHz
<input checked="" type="checkbox"/> Amateur Radio	24890kHz	24990kHz
<input checked="" type="checkbox"/> Amateur Radio	28000kHz	29700kHz

Optional Band: ☒ off ☐ Upstream ☐ Downstream

Line Type: fastOrInterleaved

Add Cancel Clear

Name	Payload Rate	SNR Margin	Applied Ports	Delete
DEFVAL	S:104M/104M , F:104M/104M	6dB/6dB	1-16	<input type="checkbox"/>

Delete Cancel

The following table describes the labels in this screen.

Table 14 VDSL Profile Setup

LABEL	DESCRIPTION
Name	Enter a descriptive name for identification purposes.
Slow Channel Payload Rate	Specifies the maximum/minimum slow channel data rate in bits/second. Enter a number between 104960 and 64.
Fast Channel Payload Rate	Specifies the maximum/minimum fast channel data rate in bits/second. Enter a number between 104960 and 64.

Table 14 VDSL Profile Setup (continued)

LABEL	DESCRIPTION
Rate Adaptive	Rate adaption is the ability of a device to adjust from the configured transmission rate to the attainable transmission rate automatically depending on the line quality. The VDSL transmission rate then stays at the new rate or adjusts if line quality improves or deteriorates. Select a rate adaptive mode. Select Manual to disable transmission rate adjustment. Select AdaptAtlnit to enable the switch to adjust to a new lower rate when the line quality deteriorates until the connection is broken.
Max SNR	Select the maximum SNR (Signal to Noise Ratio) margin allowed on the channel.
Target SNR	Select the target SNR (Signal to Noise Ratio) margin for the channel.
Min SNR	Select the minimum SNR (Signal to Noise Ratio) margin allowed on the channel.
MaxInterleave Delay	Specify maximum interleave delay for the slow channel. It is recommended that you configure the same latency delay for both downstream and upstream.
Max Aggregate Power	Specify the maximum aggregate power level for upstream and downstream transmission.
Rate Ratio	Select to use the data rate allocated for the fast or slow channel. Valid values are 0 and 100 . Enter 0 to use slow channel (at the rate you specified in the Slow Channel Payload Rate field) which is best suited for data transmission. Enter 100 to use fast channel (at the rate you specified in the Fast Channel Payload Rate field) for latency-sensitive applications (such as voice).
Impulse Noise Protection	Specify the level of impulse noise (burst) protection (in microseconds) for a slow (or interleaved) channel. Enter a number between 0 and 1275.
FEC Redundancy	This field displays the Forward Error Correction (FEC) redundancy overhead for a fast channel. This field is neither configurable nor applicable at the time of writing.
Template PSD Mask	Select a PSD mask for the upstream and downstream traffic.
PBO Control	Set the upstream PBO control. PBO (Power Back Off) allows the switch to provide better service in a network environment with telephone wiring of varying lengths. Select Disable to disable this feature. Select Auto to set the switch to automatically adjust the power backoff. Select Manual to specify a power backoff level in the PBO Level field.
PBO Level	If you select Manual in the PBO Control field, select a PBO level.
Band Plan	Specify a VDSL band plan to use for the line. Select BandPlan998 for ITU-T G.993.1 Bandplan-A and ANSI Plan 998.
Band Plan FX	This field displays the band frequency range (3750 to 12000) between the D2 and U2 bands. This field is neither configurable nor applicable at the time of writing.
Applicable Standard	Your switch automatically selects a standard to use for VDSL services.
Deployment Scenario	Specify a VDSL deployment scenario. Select FTTCab if the switch is located in a street cabinet. Select FTTEx if the switch is located at the central office (CO).

Table 14 VDSL Profile Setup (continued)

LABEL	DESCRIPTION
Compatible Mode	<p>Specify the starting band of the frequency range used by VDSL services. The end frequency band varies depending on the VDSL2 profile (frequency plan) (8a, 8b, 8c, 8d, 12a, 12b, 17a, or 30a) applied to the switch.</p> <p>This can avoid interference with other services (such as ISDN, ADSL or ADSL2 provided by other device) on the same bundle of lines.</p> <p>ISDN in Europe uses a frequency range of up to 80 kHz, while ISDN in Japan uses a frequency range of up to 640 kHz. ADSL utilizes the 1.1 MHz band. Both ADSL2 and ADSL 2+ utilize the 2.2 MHz band.</p> <p>Select None to turn on any tone (over 25 kHz). The VDSL services then use the frequency bands above 138 kHz.</p> <p>Select 640kHz to have the VDSL services use the frequency bands above 640 kHz.</p> <p>Select 1100kHz to turn off all tones below 1.1 MHz. The VDSL services then use the frequency bands above 1.1 MHz.</p> <p>Select 2200kHz to disable all tones below 2.2 MHz. The VDSL services then use the frequency bands above 2.2 MHz.</p>
Ham Band Plan	To avoid performance degradation due to RFI (Radio Frequency Interference), you can set your switch not to transmit signals in the pre-defined HAM (Handheld Amateur Radio) radio band(s).
Optional Band	<p>Specify whether the switch is to use the optional band for the upstream traffic.</p> <p>For POTS, the optional bands range from 25 to 138 K.</p> <p>For ISDN, the optional bands range from 138 - 276 K.</p> <p>The optional bands are not supported in a VDSL1 device.</p>
Line Type	This displays the VDSL line type (fastOrInterleaved), that means either fast or interleaved channel exists, but only one works at a time.
Add	Click Add to save the new profile to the switch. It then displays in the summary table at the bottom of the screen.
Cancel	Click Cancel to reset the fields to your previous configuration.
Clear	Click Clear to clear the fields to the factory defaults.
Name	This field displays the descriptive name for this profile.
Payload Rate	This field displays the configured maximum upstream and downstream payload rates in megabits per second.
SNR Margin	This field displays the configured upstream and downstream signal to noise ration in decibels.
Applied Ports	<p>You can apply a profile to a VDSL port in the Port Setup screen.</p> <p>This field displays the VDSL port number(s) to which this profile is applied.</p>
Delete	Check the rule(s) that you want to remove in the Delete column and then click the Delete button.
Cancel	Click Cancel to clear the selected checkboxes in the Delete column.

6.10 VDSL Alarm Profile Setup

Alarm profiles define VDSL port alarm thresholds. The device sends an alarm trap and generates a syslog entry when the thresholds of the alarm profile are exceeded.

Click **Basic Settings** and **VDSL Alarm Profile Setup** in the navigation panel to display the screen as shown.

Figure 25 VDSL Alarm Profile Setup

VDSL Alarm Profile Setup

Name	DEFVAL
15 Minute LOFs Threshold	0
15 Minute LOSs Threshold	0
15 Minute LPRs Threshold	0
15 Minute LOLs Threshold	0
15 Minute ESs Threshold	0
15 Minute SESSs Threshold	0
15 Minute UASs Threshold	0
Initialization Failure	Off

Add Cancel Clear

Name	LOSs	ESs	SESSs	Init	Applied Ports	Delete
DEFVAL	0	0	0	Off	1-16	

Delete Cancel

The following table describes the labels in this screen.

Table 15 VDSL Alarm Profile Setup

LABEL	DESCRIPTION
Name	Enter a descriptive name for identification purposes.
15 Minute LOFs Threshold	Enter the number of Loss Of Framing seconds (LOFs) that are permitted to occur within 15 minutes.
15 Minute LOSs Threshold	Enter the number of Loss Of Signals seconds (LOSs) that are permitted to occur within 15 minutes.
15 Minute LPRs Threshold	Enter the number of Loss of PowerR seconds (LPRs) is permitted to occur within 15 minutes.
15 Minute LOLs Threshold	Enter the number of Loss Of Link seconds (LOLs) that are permitted to occur within 15 minutes.
15 Minute ESs Threshold	Enter the number of Errored Seconds (ESs) that are permitted to occur within 15 minutes.
15 Minute SESSs Threshold	Enter the number of Severely Errored Seconds (SESSs) that are permitted to occur within 15 minutes.
15 Minute UASs Threshold	Enter the number of UnAvailable Seconds (UASs) that are permitted to occur within 15 minutes.
Initialization Failure	Select On to trigger an alarm for an initialization failure trap. Select Off to disable trap sending when a line fails to initialize.
Add	Click Add to save the new rule to the switch. It then displays in the summary table at the bottom of the screen.
Cancel	Click Cancel to reset the fields to your previous configuration.
Clear	Click Clear to clear the fields to the factory defaults.
Name	This field displays the descriptive name for the alarm profile.
LOSs	This field displays the number of Loss Of Signal (LOS) seconds that are permitted to occur within 15 minutes.
ESs	This field displays the number of Errored Seconds (ESs) that are permitted to occur within 15 minutes.

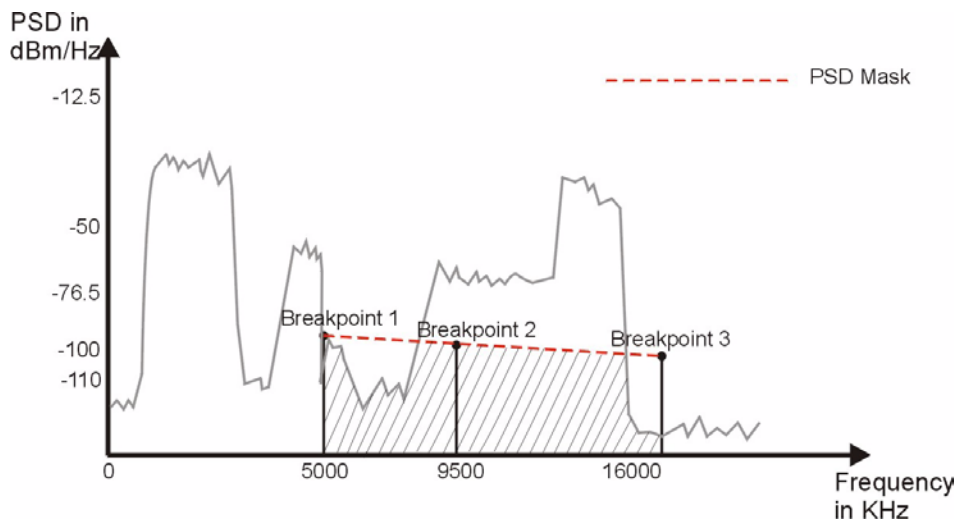
Table 15 VDSL Alarm Profile Setup (continued)

LABEL	DESCRIPTION
SESSs	This field displays the number of Severely Errored Seconds (SESSs) that are permitted to occur within 15 minutes.
Init	This field displays whether the initialization failure trap sending feature is enabled (On) or not (Off).
Applied Ports	You can apply a profile to a VDSL port in the Port Setup screen. This field displays the VDSL port number(s) to which this profile is applied.
Delete	Check the rule(s) that you want to remove in the Delete column and then click the Delete button.
Cancel	Click Cancel to clear the selected checkboxes in the Delete column.

6.11 VDSL PSD Profile Setup

PSD (Power Spectral Density) profiles define the allowable downstream and upstream PSD values for a line. In a PSD profile, you can configure a set of breakpoints, each of which is defined by a frequency and PSD level. The set of breakpoints forms a PSD mask that specifies the maximum transmission power of each VDSL frequency band. If the frequency range used by the Switch and other devices overlap, you can configure the PSD of your Switch to prevent interference with other nearby signals.

In the following example, the Switch's PSD is configured to not exceed the PSD mask (dashed line) within the 5 MHz to 16 MHz frequency range. After configuration, the shaded area is the Switch's actual PSD for the specified frequency range.

Figure 26 PSD-Frequency Example

Click **Basic Settings** and **VDSL PSD Profile Setup** in the navigation panel to display the screen as shown.

Figure 27 VDSL PSD Profile Setup

The following table describes the labels in this screen.

Table 16 VDSL PSD Profile Setup

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for identification purposes. This field is configurable only when you click the Add New Profile link.
Add New Profile	Click this link to add a new profile.
Add	Click Add to save the new profile to the Switch. It then displays in the summary table at the bottom of the screen.
Down Stream / Up Stream	
Tone Freq	Enter a downstream or upstream tone frequency between 0 and 30000 (in kHz).
PSD Level (dBm/Hz)	Specify a downstream or upstream PSD value between 125 and 1400 in units of -0.1 dBm/Hz. For example, if you want to set the transmit power to -20 dBm/Hz, enter 200.
Add	Click Add to save the new breakpoint to the Switch. It then displays in the summary table in the center of the screen.
BreakPoint	This is the index number of each breakpoint.
Tone Freq	This displays the tone frequency for this breakpoint.
PSD Level (dBm/Hz)	This displays the transmit power for this breakpoint.
Delete	Check the breakpoint(s) that you want to remove in the Delete column and then click the Delete button.
Profile Name	This field displays the descriptive name for this profile.
Applied Ports	You can apply a profile to a VDSL port in the Port Setup screen. This field displays the VDSL port number(s) to which this profile is applied.
Delete	Check the profile(s) that you want to remove in the Delete column and then click the Delete button.
Cancel	Click Cancel to clear the selected checkboxes in the Delete column.

PART III

Advanced

VLAN (87)
Static MAC Forward Setup (97)
Filtering (99)
Spanning Tree Protocol (101)
Bandwidth Control (107)
Broadcast Storm Control (109)
Mirroring (111)
Link Aggregation (113)
Port Authentication (117)
Port Security (121)
Queuing Method (123)
Classifier (127)
Policy (133)
VLAN Stacking (139)
Multicast (145)
Differentiated Services (157)

The type of screen you see here depends on the **VLAN Type** you selected in the **Switch Setup** screen. This chapter shows you how to configure 802.1Q tagged and port-based VLANs.

7.1 Introduction to IEEE 802.1Q Tagged VLAN

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier), residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information), starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

TPID 2 Bytes	User Priority 3 Bits	CFI 1 Bit	VLAN ID 12 Bits
-----------------	-------------------------	--------------	--------------------

7.1.1 Forwarding Tagged and Untagged Frames

Each port on the switch is capable of passing tagged or untagged frames. To forward a frame from an 802.1Q VLAN-aware switch to an 802.1Q VLAN-unaware switch, the switch first decides where to forward the frame and then strips off the VLAN tag. To forward a frame from an 802.1Q VLAN-unaware switch to an 802.1Q VLAN-aware switch, the switch first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID. The default PVID is VLAN 1 for all ports, but this can be changed.

7.2 Automatic VLAN Registration

GARP and GVRP are the protocols used to automatically register VLAN membership across switches.

7.2.1 GARP

GARP (Generic Attribute Registration Protocol) allows network switches to register and de-register attribute values with other GARP participants within a bridged LAN. GARP is a protocol that provides a generic mechanism for protocols that serve a more specific application, for example, GVRP.

7.2.1.1 GARP Timers

Switches join VLANs by making a declaration. A declaration is made by issuing a Join message using GARP. Declarations are withdrawn by issuing a Leave message. A Leave All message terminates all registrations. GARP timers set declaration timeout values.

7.2.2 GVRP

GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network. Enable this function to permit VLANs groups beyond the local switch.

Table 17 IEEE 802.1Q Terminology

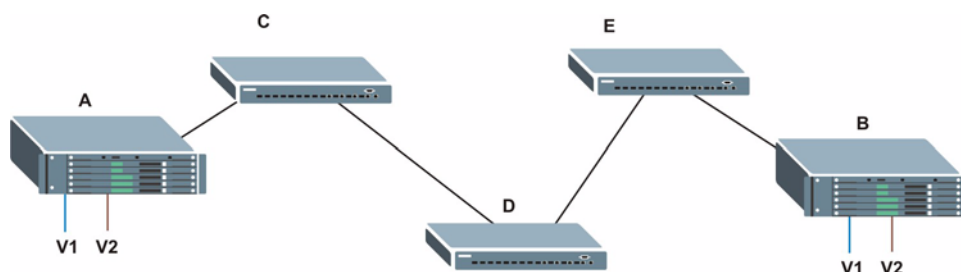
VLAN PARAMETER	TERM	DESCRIPTION
VLAN Type	Permanent VLAN	This is a static VLAN created manually.
	Dynamic VLAN	This is a VLAN configured by a GVRP registration/deregistration process.
VLAN Administrative Control	Registration Fixed	Fixed registration ports are permanent VLAN members.
	Registration Forbidden	Ports with registration forbidden are forbidden to join the specified VLAN.
	Normal Registration	Ports dynamically join a VLAN using GVRP.
VLAN Tag Control	Tagged	Ports belonging to the specified VLAN tag all outgoing frames transmitted.
	Untagged	Ports belonging to the specified don't tag all outgoing frames transmitted.
VLAN Port	Port VID	This is the VLAN ID assigned to untagged frames that this port received.
	Acceptable frame type	You may choose to accept both tagged and untagged incoming frames or just tagged incoming frames on a port.
	Ingress filtering	If set, the switch discards incoming frames for VLANs that do not have this port as a member

7.3 Port VLAN Trunking

Enable **VLAN Trunking** on a port to allow frames belonging to unknown VLAN groups to pass through that port. This is useful if you want to set up VLAN groups on end devices without having to configure the same VLAN groups on intermediary devices.

Refer to the following figure. Suppose you want to create VLAN groups 1 and 2 (V1 and V2) on devices A and B. Without **VLAN Trunking**, you must configure VLAN groups 1 and 2 on all intermediary switches C, D and E; otherwise they will drop frames with unknown VLAN group tags. However, with **VLAN Trunking** enabled on a port(s) in each intermediary switch you only need to create VLAN groups in the end devices (A and B). C, D and E automatically allow frames with VLAN group tags 1 and 2 (VLAN groups that are unknown to those switches) to pass through their VLAN trunking port(s).

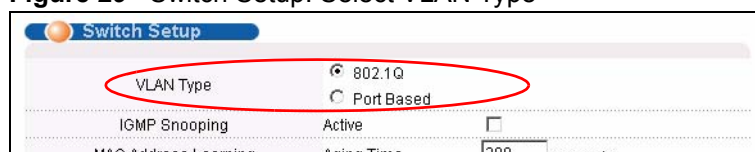
Figure 28 Port VLAN Trunking



7.4 Select the VLAN Type

Select a VLAN type in the **Switch Setup** screen.

Figure 29 Switch Setup: Select VLAN Type



7.5 Static VLAN

Use a static VLAN to decide whether an incoming frame on a port should be

- sent to a VLAN group as normal depends on its VLAN tag.
- sent to a group whether it has a VLAN tag or not.
- blocked from a VLAN group regardless of its VLAN tag.

You can also tag all outgoing frames (that were previously untagged) from a port with the specified VID.

7.5.1 Static VLAN Status

Click **Advanced Application > VLAN** from the navigation panel to display the **VLAN Status** screen as shown next.

Use this screen to view the current static VLAN group(s) you have configured. Refer to [Section 7.1 on page 87](#) for background information.

Figure 30 VLAN > VLAN Status

Index	VID	Port Number									Elapsed Time	Status
		2	4	6	8	10	12	14	16	18		
1	1	U	U	U	U	U	U	U	U	U	1:35:54	Static

Poll Interval(s):

Change Pages:

The following table describes the labels in this screen.

Table 18 VLAN > VLAN Status

LABEL	DESCRIPTION
The Number of VLAN	This is the number of VLANs configured on the switch.
Index	This is the VLAN index number.
VID	This is the VLAN identification number that was configured in the Static VLAN screen.
Port Number	This column displays the ports that are participating in a VLAN. A tagged port is marked as T , an untagged port is marked as U and ports not participating in a VLAN in marked as — .
Elapsed Time	This field shows how long it has been since a normal VLAN was registered or a static VLAN was set up.
Status	This field shows how this VLAN was added to the switch; dynamic - using GVRP, static - added as a permanent entry or other - added using Multicast VLAN Registration (MVR).
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking Set Interval .
Stop	Click Stop to halt polling statistics.
Change Pages	Click Previous Page or Next Page to show the previous/next screen if all status information cannot be seen in one screen.

7.5.2 Configure a Static VLAN

To configure a static VLAN, click **Static VLAN** in the **VLAN Status** screen to display the screen as shown next.

Use a static VLAN to decide whether an incoming frame on a port should be

- sent to a VLAN group as normal depends on its VLAN tag.
- sent to a group whether it has a VLAN tag or not.
- blocked from a VLAN group regardless of its VLAN tag.

You can also tag all outgoing frames (that were previously untagged) from a port with the specified VID. Refer to [Section 7.1 on page 87](#) for background information.

Figure 31 VLAN > Static VLAN

The screenshot shows the 'Static VLAN' configuration interface. At the top, there's a title bar with 'Static VLAN' and a 'VLAN Status' link. Below this is an 'ACTIVE' checkbox. There are input fields for 'Name' and 'VLAN Group ID'. The main part of the screen is a table for configuring ports. The table has three columns: 'Port', 'Control', and 'Tagging'. The 'Control' column has three radio button options: 'Normal' (selected), 'Fixed', and 'Forbidden'. The 'Tagging' column has a checkbox for 'Tx Tagging', which is checked for all ports. The ports listed are 1, 2, 3, 4, 16, 17, and 18. Below the table are three buttons: 'Add', 'Cancel', and 'Clear'. At the bottom of the screen is a summary table with four columns: 'VID', 'Active', 'Name', and 'Delete'. The first row shows VID 1, Active Yes, Name 1, and a delete checkbox. Below this summary table are 'Delete' and 'Cancel' buttons.

The following table describes the related labels in this screen.

Table 19 VLAN > Static VLAN

LABEL	DESCRIPTION
ACTIVE	Select this check box to activate the VLAN settings.
Name	Enter a descriptive name for the VLAN group for identification purposes.
VLAN Group ID	Enter the VLAN ID for this static VLAN; the valid range is between 1 and 4094.
Port	The port number identifies the port you are configuring.
Control	Select Normal for the port to dynamically join this VLAN group using GVRP. This is the default selection. Select Fixed for the port to be a permanent member of this VLAN group. Select Forbidden if you want to prohibit the port from joining this VLAN group.
Tagging	Select TX Tagging if you want the port to tag all outgoing frames (that were previously untagged) transmitted with this VLAN Group ID.
Add	Click Add to add the settings as a new entry in the summary table below.

Table 19 VLAN > Static VLAN (continued)

LABEL	DESCRIPTION
Cancel	Click Cancel to reset the fields.
Clear	Click Clear to start configuring the screen again.
VID	This field displays the ID number of the VLAN group. Click the number to edit the VLAN settings.
Active	This field indicates whether the VLAN settings are enabled (Yes) or disabled (No).
Name	This field displays the descriptive name for this VLAN group.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

7.5.3 Configure VLAN Port Setting

To configure the VLAN settings on a port, click the **VLAN Port Setting** link in the **VLAN Status** screen. Refer to [Section 7.1 on page 87](#) for background information.

Figure 32 VLAN > VLAN Port Setting

Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking
1	<input checked="" type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
2	<input checked="" type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
...
15	<input checked="" type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
16	<input checked="" type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
17	<input checked="" type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
18	<input checked="" type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>

The following table describes the labels in this screen.

Table 20 VLAN > VLAN Port Setting

label	description
GVRP	GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network. Select this check box to permit VLAN groups beyond the local switch.
Port Isolation	Port Isolation allows each port to communicate only with the CPU management port and the uplink ports but not communicate with each other. This option is the most limiting but also the most secure.
Port	This field displays the port number.
Ingress Check	Select this check box to discard incoming frames for VLANs that do not have this port as a member. Clear this check box to disable ingress filtering.
PVID	Enter a number between 1 and 4094 as the port VLAN ID.

Table 20 VLAN > VLAN Port Setting (continued)

label	description
GVRP	Select this check box to allow GVRP on this port.
Acceptable Frame Type	Specify the type of frames allowed on a port. Choices are All , Tag Only and Untag Only . Select All to accept all untagged or tagged frames on this port. This is the default setting. Select Tag Only to accept only tagged frames on this port. All untagged frames will be dropped. Select Untag Only to accept only untagged frames on this port. All tagged frames will be dropped.
VLAN Trunking	Enable VLAN Trunking on ports connected to other switches or routers (but not ports directly connected to end users) to allow frames belonging to unknown VLAN groups to pass through the switch.
Apply	Click Apply to save the changes
Cancel	Click Cancel to start configuring the screen again.

7.6 Port-based VLAN

Port-based VLANs are VLANs where the packet forwarding decision is based on the destination MAC address and its associated port.

Port-based VLANs require allowed outgoing ports to be defined for each port. Therefore, if you wish to allow two subscriber ports to talk to each other, for example, between conference rooms in a hotel, you must define the egress (an egress port is an outgoing port, that is, a port through which a data packet leaves) for both ports.

Port-based VLANs are specific only to the switch on which they were created.



When you activate port-based VLAN, the switch uses a default VLAN ID of 1. You cannot change it.



In screens (such as **IP Setup** and **Filtering**) that require a VID, you must enter 1 as the VID.

The port-based VLAN setup screen is shown next. The **CPU** management port forms a VLAN with all Ethernet ports.

7.6.1 Configure a Port-based VLAN

Select **Port Based** as the **VLAN Type** in the **Switch Setup** screen (see [Figure 29 on page 89](#)) and then click **VLAN** from the navigation panel to display the next screen.

Figure 33 Port Based VLAN Setup (All Connected)

Port Based VLAN Setup

Setting Wizard

All connected

Set

Incoming

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1
2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2
3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3
4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	4
5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	5
6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	6
7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	7
8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	8
9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9
10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	10
11	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	11
12	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	12
13	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	13
14	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	14
15	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	15
16	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	16
17	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	17
18	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	18
CPU	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	CPU
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	

Outgoing

Apply

Cancel

Figure 34 Port Based VLAN Setup (Port Isolation)

Setting Wizard: **Port isolation** **Set**

Incoming

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
13	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
14	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
15	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
16	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
17	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
18	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
CPU	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Outgoing

Apply **Cancel**

The following table describes the labels in this screen.

Table 21 Port Based VLAN Setup

LABEL	DESCRIPTION
Setting Wizard	<p>Choose All connected or Port isolation.</p> <p>All connected means all ports can communicate with each other, that is, there are no virtual LANs. All incoming and outgoing ports are selected. This option is the most flexible but also the least secure.</p> <p>Port isolation means that each port can only communicate with the CPU management port and cannot communicate with each other. All incoming ports are selected while only the CPU outgoing port is selected. This option is the most limiting but also the most secure.</p> <p>After you make your selection, click Set (top right of screen) to display the screens as mentioned above. You can still customize these settings by adding/deleting incoming or outgoing ports, but you must also click Apply at the bottom of the screen.</p>
Incoming	<p>These are the ingress ports; an ingress port is an incoming port, that is, a port through which a data packet enters. If you wish to allow two subscriber ports to talk to each other, you must define the ingress port for both ports. The numbers in the top row denote the incoming port for the corresponding port listed on the left (its outgoing port). CPU refers to the switch management port. By default it forms a VLAN with all Ethernet ports. If it does not form a VLAN with a particular port then the switch cannot be managed from that port.</p>
Outgoing	<p>These are the egress ports; an egress port is an outgoing port, that is, a port through which a data packet leaves. If you wish to allow two subscriber ports to talk to each other, you must define the egress port for both ports. CPU refers to the switch management port. By default it forms a VLAN with all Ethernet ports. If it does not form a VLAN with a particular port then the switch cannot be managed from that port.</p>

Table 21 Port Based VLAN Setup (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save the changes.
Cancel	Click Cancel to start configuring the screen again.

Static MAC Forward Setup

Use these screens to configure static MAC address forwarding.

8.1 Static MAC Forwarding Overview

A static MAC address is an address that has been manually entered in the MAC address learning table. Static MAC addresses do not age out. When you set up static MAC address rules, you are setting static MAC addresses for a port. This may reduce the need for broadcasting.

8.2 Configuring Static MAC Forwarding

Click **Advanced Applications > Static MAC Forwarding** in the navigation panel to display the configuration screen as shown. Scroll down to the bottom of the screen to view the summary table for the settings.

Figure 35 Static MAC Forwarding

Index	Active	Name	MAC Address	VID	Port	Delete
1	No	Example	00:b2:a0:9e:f0:3c	2	1	<input type="checkbox"/>

The following table describes the labels in this screen.

Table 22 Static MAC Forwarding

LABEL	DESCRIPTION
Active	Select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by clearing this check box.
Name	Enter a descriptive name for identification purposes for this static MAC address forwarding rule.

Table 22 Static MAC Forwarding (continued)

LABEL	DESCRIPTION
MAC Address	Enter the MAC address in valid MAC address format, that is, six hexadecimal character pairs. Note: Static MAC addresses do not age out.
VID	Enter the VLAN identification number.
Port	Select a port where the MAC address entered in the previous field will be automatically forwarded.
Add	After you set the fields above, click Add to insert a new rule.
Cancel	Click Cancel to reset the fields.
Clear	Click Clear to begin configuring this screen afresh.
Index	Click an index number to modify the settings.
Active	This field displays whether this static MAC address forwarding rule is active (Yes) or not (No). You may temporarily deactivate a rule without deleting it.
Name	This field displays the descriptive name for identification purposes for this static MAC address-forwarding rule.
MAC Address	This field displays the MAC address that will be forwarded and the VLAN identification number to which the MAC address belongs.
VID	This field displays the VLAN identification number to which the MAC address belongs.
Port	This field displays the port where the MAC address shown in the next field will be forwarded.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

Filtering

This chapter discusses static IP and MAC address port filtering.

9.1 Filtering Overview

Filtering means sifting traffic going through the switch based on the source and/or destination MAC addresses and VLAN group (ID).

9.2 Configure a Filtering Rule

Click **Advanced Application > Filtering** in the navigation panel to display the screen as shown next. Scroll down to the bottom of the screen to view the summary table for the settings.

Figure 36 Filtering

The following table describes the related labels in this screen.

Table 23 Filtering

LABEL	DESCRIPTION
Active	Make sure to select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by deselecting this check box.
Name	Type a descriptive name for this filter rule. This is for identification purpose only.

Table 23 Filtering (continued)

LABEL	DESCRIPTION
Action	<p>Select Discard source to drop frame from the source MAC address (specified in the MAC field). The switch can still send frames to the MAC address.</p> <p>Select Discard destination to drop frames to the destination MAC address (specified in the MAC field). The switch can still receive frames originating from the MAC address.</p> <p>Select Discard source and Discard destination to block traffic to/from the MAC address specified in the MAC field.</p>
MAC	Type a MAC address in valid MAC address format, that is, six hexadecimal character pairs.
VID	Type the VLAN group identification number.
Add	Click Add to save the new rule to the switch. It then displays in the summary table at the bottom of the screen.
Cancel	Click Cancel to reset the fields to your previous configuration.
Clear	Click Clear to clear the fields to the factory defaults.
Index	This field displays the index number of the rule. Click an index number to change the settings.
Active	This field displays Yes when the rule is activated and No when is it deactivated.
Name	This field displays the descriptive name for this rule. This is for identification purpose only.
MAC Address	This field displays the source/destination MAC address with the VLAN identification number to which the MAC address belongs.
Action	This field displays the filter action.
Delete	Check the rule(s) that you want to remove in the Delete column and then click the Delete button.
Cancel	Click Cancel to clear the selected checkbox(es) in the Delete column.

Spanning Tree Protocol

This chapter introduces the Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP).

10.1 STP/RSTP Overview

(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a switch to interact with other (R)STP -compliant switches in your network to ensure that only one path exists between any two stations on the network.

The switch uses IEEE 802.1w RSTP (Rapid Spanning Tree Protocol) that allows faster convergence of the spanning tree than STP (while also being backwards compatible with STP-only aware bridges). In RSTP, topology change information is directly propagated throughout the network from the device that generates the topology change. In STP, a longer delay is required as the device that causes a topology change first notifies the root bridge that then notifies the network. Both RSTP and STP flush unwanted learned addresses from the filtering database. In RSTP, the port states are Discarding, Learning, and Forwarding.



In this user's guide, "STP" refers to both STP and RSTP.

10.1.1 STP Terminology

The root bridge is the base of the spanning tree; it is the bridge with the lowest identifier value (MAC address).

Path cost is the cost of transmitting a frame onto a LAN through that port. It is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost.

Table 24 STP Path Costs

	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	4Mbps	250	100 to 1000	1 to 65535
Path Cost	10Mbps	100	50 to 600	1 to 65535
Path Cost	16Mbps	62	40 to 400	1 to 65535

Table 24 STP Path Costs

	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	100Mbps	19	10 to 60	1 to 65535
Path Cost	1Gbps	4	3 to 10	1 to 65535
Path Cost	10Gbps	2	1 to 5	1 to 65535

On each bridge, the root port is the port through which this bridge communicates with the root. It is the port on this switch with the lowest path cost to the root (the root path cost). If there is no root port, then this switch has been accepted as the root bridge of the spanning tree network.

For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.

10.1.2 How STP Works

After a bridge determines the lowest cost-spanning tree with STP, it enables the root port and the ports that are the designated ports for connected LANs, and disables all other ports that participate in STP. Network packets are therefore only forwarded between enabled ports, eliminating any possible network loops.

STP-aware switches exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridged LAN topology changes, a new spanning tree is constructed.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

10.1.3 STP Port States

STP assigns five port states to eliminate packet looping. A bridge port is not allowed to go directly from blocking state to forwarding state so as to eliminate transient loops.

Table 25 STP Port States

PORT STATE	DESCRIPTION
Disabled	STP is disabled (default).
Blocking	Only configuration and management BPDUs are received and processed.
Listening	All BPDUs are received and processed.
Learning	All BPDUs are received and processed. Information frames are submitted to the learning process but not forwarded.
Forwarding	All BPDUs are received and processed. All information frames are received and forwarded.

10.2 STP Status

Click **Advanced Application > Spanning Tree Protocol** in the navigation panel to display the screen. View current STP status on the switch in this screen.

Refer to [Section 10.1 on page 101](#) for background information.

Figure 37 Spanning Tree Protocol Status

Spanning Tree Protocol Status [Configuration](#)

Spanning Tree Protocol : Running

Bridge	Root	Our Bridge
Bridge ID	8000-001349038297	8000-001349038297
Hello Time (second)	2	2
Max Age (second)	20	20
Forwarding Delay (second)	15	15
Cost to Bridge	0	
Port ID	0X0000	
Topology Changed Times		0
Time Since Last Change		0:00:10

Polling Interval: Set Interval Stop

The following table describes the labels in this screen.

Table 26 Spanning Tree Protocol Status

LABEL	DESCRIPTION
Spanning Tree Protocol	This field displays Running if STP is activated. Otherwise, it displays Down .
Configuration	Click Configuration to configure STP settings. Refer to Section 10.3 on page 104 .
Bridge	Root refers to the base of the spanning tree (the root bridge). Our Bridge is this switch. This switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for Root and Our Bridge if the switch is the root switch.
Hello Time (second)	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines Hello Time , Max Age and Forwarding Delay .
Max Age (second)	This is the maximum time (in seconds) a switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding).
Cost to Bridge	This is the path cost from the root port on this switch to the root switch.
Port ID	This is the priority and number of the port on the switch through which this switch must communicate with the root of the Spanning Tree.

Table 26 Spanning Tree Protocol Status (continued)

LABEL	DESCRIPTION
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking Set Interval .
Stop	Click Stop to halt STP statistic polling.

10.3 Configure STP

To configure STP, click the **Configuration** link in the **Spanning Tree Protocol** screen as shown next. Refer to [Section 10.1 on page 101](#) for background information.

Figure 38 Spanning Tree Protocol > Configuration

Spanning Tree Protocol Status

Active ☒

Bridge Priority

Hello Time Seconds

Max Age Seconds

Forwarding Delay Seconds

Port	Active	Priority	Path Cost
17	<input checked="" type="checkbox"/>	<input type="text" value="128"/>	<input type="text" value="4"/>
18	<input checked="" type="checkbox"/>	<input type="text" value="128"/>	<input type="text" value="4"/>

Apply Cancel

The following table describes the labels in this screen.

Table 27 Spanning Tree Protocol > Configuration

LABEL	DESCRIPTION
Status	Click Status to display the Spanning Tree Protocol Status screen.
Active	Select this check box to activate STP. Clear this checkbox to disable STP.
Bridge Priority	Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Select a value from the drop-down list box. The lower the numeric value you assign, the higher the priority for this bridge. Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.

Table 27 Spanning Tree Protocol > Configuration (continued)

LABEL	DESCRIPTION
Max Age	This is the maximum time (in seconds) a switch can wait without receiving a BPDU before attempting to reconfigure. All switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the switch ports attached to the network. The allowed range is 6 to 40 seconds.
Forwarding Delay	This is the maximum time (in seconds) a switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: $2 * (\text{Forward Delay} - 1) \geq \text{Max Age} \geq 2 * (\text{Hello Time} + 1)$
Port	This field displays the port number.
Active	Select this check box to activate STP on this port.
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and the default value is 128.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is assigned according to the speed of the bridge. The slower the media, the higher the cost - see Table 24 on page 101 for more information.
Apply	Click Apply to save your changes back to the switch.
Cancel	Click Cancel to begin configuring this screen afresh.

Bandwidth Control

This chapter shows you how you can cap the maximum bandwidth allowed on the ports using the **Bandwidth Control** screen.

11.1 Configuring Bandwidth Control

Bandwidth control means defining a maximum allowable bandwidth for incoming and/or outgoing traffic on a port.

11.1.1 CIR and PIR

The Committed Information Rate (CIR) is the guaranteed bandwidth for the incoming traffic flow on a port. The Peak Information Rate (PIR) is the maximum bandwidth allowed for the incoming traffic flow on a port when there is no network congestion.

The CIR and PIR should be set for all ports that use the same uplink bandwidth. If the CIR is reached, packets are sent at the rate up to the PIR. When network congestion occurs, packets through the ingress port exceeding the CIR will be marked for drop.



The CIR should be less than the PIR.



The sum of CIRs cannot be greater than or equal to the uplink bandwidth.

Click **Advanced Application** and then **Bandwidth Control** in the navigation panel to bring up the screen as shown next.

Figure 39 Bandwidth Control

Port	Active	Ingress Rate		Egress Rate
		Commit Rate	Peak Rate	
1	<input type="checkbox"/>	1 Kbps	1 Kbps	1 Kbps
2	<input type="checkbox"/>	1 Kbps	1 Kbps	1 Kbps
3	<input type="checkbox"/>	1 Kbps	1 Kbps	1 Kbps
4	<input type="checkbox"/>	1 Kbps	1 Kbps	1 Kbps
5	<input type="checkbox"/>	1 Kbps	1 Kbps	1 Kbps
6	<input type="checkbox"/>	1 Kbps	1 Kbps	1 Kbps
7	<input type="checkbox"/>	1 Kbps	1 Kbps	1 Kbps
8	<input type="checkbox"/>	1 Kbps	1 Kbps	1 Kbps
9	<input type="checkbox"/>	1 Kbps	1 Kbps	1 Kbps
10	<input type="checkbox"/>	1 Kbps	1 Kbps	1 Kbps
11	<input type="checkbox"/>	1 Kbps	1 Kbps	1 Kbps
12	<input type="checkbox"/>	1 Kbps	1 Kbps	1 Kbps
13	<input type="checkbox"/>	1 Kbps	1 Kbps	1 Kbps
14	<input type="checkbox"/>	1 Kbps	1 Kbps	1 Kbps
15	<input type="checkbox"/>	1 Kbps	1 Kbps	1 Kbps
16	<input type="checkbox"/>	1 Kbps	1 Kbps	1 Kbps
17	<input type="checkbox"/>	1 Kbps	1 Kbps	1 Kbps
18	<input type="checkbox"/>	1 Kbps	1 Kbps	1 Kbps

Apply Cancel

The following table describes the related labels in this screen.

Table 28 Bandwidth Control

LABEL	DESCRIPTION
Active	Select this check box to enable bandwidth control on the switch.
Port	This field displays the port number.
Active	Make sure to select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by deselecting this check box.
Ingress Rate	
Commit Rate	Specify the guaranteed bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on a port. The commit rate should be less than the peak rate. The sum of commit rates cannot be greater than or equal to the uplink bandwidth.
Peak Rate	Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on a port.
Egress Rate	Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the out-going traffic flow on a port. Enter a number between 1000 and 1000 000.
Apply	Click Apply to save the settings.
Cancel	Click Cancel to reset the fields to your previous configuration.

Broadcast Storm Control

This chapter introduces and shows you how to configure the broadcast storm control feature.

12.1 Broadcast Storm Control Overview

Broadcast storm control limits the number of broadcast, multicast and destination lookup failure (DLF) packets the switch receives per second on the ports. When the maximum number of allowable broadcast, multicast and/or DLF packets is reached per second, the subsequent packets are discarded. Enable this feature to reduce broadcast, multicast and/or DLF packets in your network. You can specify limits for each packet type on each port.

12.2 Broadcast Storm Control Setup

Click **Advanced Application > Broadcast Storm Control** in the navigation panel to display the screen as shown next.

Figure 40 Broadcast Storm Control

Port	Broadcast (pkt/s)	Multicast (pkt/s)	DLF (pkt/s)
1	<input type="checkbox"/> 0	<input type="checkbox"/> 0	<input type="checkbox"/> 0
2	<input type="checkbox"/> 0	<input type="checkbox"/> 0	<input type="checkbox"/> 0
3	<input type="checkbox"/> 0	<input type="checkbox"/> 0	<input type="checkbox"/> 0
15	<input type="checkbox"/> 0	<input type="checkbox"/> 0	<input type="checkbox"/> 0
16	<input type="checkbox"/> 0	<input type="checkbox"/> 0	<input type="checkbox"/> 0
17	<input type="checkbox"/> 0	<input type="checkbox"/> 0	<input type="checkbox"/> 0
18	<input type="checkbox"/> 0	<input type="checkbox"/> 0	<input type="checkbox"/> 0

The following table describes the labels in this screen.

Table 29 Broadcast Storm Control

LABEL	DESCRIPTION
Active	Select this check box to enable broadcast storm control on the switch.
Port	This field displays a port number.

Table 29 Broadcast Storm Control (continued)

LABEL	DESCRIPTION
Broadcast (pkt/s)	Select this option and specify how many broadcast packets the port receives per second.
Multicast (pkt/s)	Select this option and specify how many multicast packets the port receives per second.
DLF (pkt/s)	Select this option and specify how many destination lookup failure (DLF) packets the port receives per second.
Apply	Click Apply to save your changes back to the switch.
Cancel	Click Cancel to begin configuring this screen afresh.

Mirroring

This chapter shows you how to configure mirroring on the switch.

13.1 Mirroring Overview

Port mirroring allows you to copy a traffic flow to a monitor port (the port you copy the traffic to) in order that you can examine the traffic from the monitor port without interference.

13.2 Port Mirroring Configuration

Click **Advanced Application > Mirroring** in the navigation panel to display the configuration screen.

Use this screen to select a monitor port and specify the traffic flow to be copied to the monitor port

Figure 41 Mirroring

Port	Mirrored	Direction
1	<input type="checkbox"/>	Ingress
2	<input type="checkbox"/>	Ingress
3	<input type="checkbox"/>	Ingress
4	<input type="checkbox"/>	Ingress
15	<input type="checkbox"/>	Ingress
16	<input type="checkbox"/>	Ingress
17	<input type="checkbox"/>	Ingress
18	<input type="checkbox"/>	Ingress

The following table describes the related labels in this screen.

Table 30 Mirroring

LABEL	DESCRIPTION
Active	Clear this check box to deactivate port mirroring on the switch.
Monitor Port	The monitor port is the port you copy the traffic to in order to examine it in more detail without interfering with the traffic flow on the original port(s). Select this port from this drop-down list box.
Port	This field displays the port number.
Mirrored	Select this option to mirror the traffic on a port.
Direction	Specify the direction of the traffic to mirror. Choices are Egress (outgoing), Ingress (incoming) and Both .
Apply	Click Apply to save the changes.
Cancel	Click Cancel to start configuring the screen again.

Link Aggregation

This chapter shows you how to logically aggregate physical links to form one logical, higher-bandwidth link.

14.1 Link Aggregation Overview

Link aggregation (trunking) is the grouping of physical ports into one logical higher-capacity link. You may want to trunk ports if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link.

However, the more ports you aggregate then the fewer available ports you have. A trunk group is one logical link containing multiple ports.

14.1.1 Dynamic Link Aggregation

The switch adheres to the IEEE 802.3ad standard for static and dynamic (LACP) port trunking.

The switch supports the link aggregation IEEE802.3ad standard. This standard describes the Link Aggregate Control Protocol (LACP), which is a protocol that dynamically creates and manages trunk groups.

When you enable LACP link aggregation on a port, the port can automatically negotiate with the ports at the remote end of a link to establish trunk groups. LACP also allows port redundancy, that is, if an operational port fails, then one of the “standby” ports become operational without user intervention. Please note that:

- You must connect all ports point-to-point to the same Ethernet switch and configure the ports for LACP trunking.
- LACP only works on full-duplex links.
- All ports in the same trunk group must have the same media type, speed, duplex mode and flow control settings.

Configure trunk groups or LACP before you connect the Ethernet switch to avoid causing network topology loops.

14.1.2 Link Aggregation ID

LACP aggregation ID consists of the following information¹:

Table 31 Link Aggregation ID: Local Switch

SYSTEM PRIORITY	MAC ADDRESS	KEY	PORT PRIORITY	PORT NUMBER
0000	00-00-00-00-00	0000	00	0000

Table 32 Link Aggregation ID: Peer Switch

SYSTEM PRIORITY	MAC ADDRESS	KEY	PORT PRIORITY	PORT NUMBER
0000	00-00-00-00-00	0000	00	0000

14.2 Link Aggregation Status

Click **Advanced Application > Link Aggregation** in the navigation panel. The **Link Aggregation Control Protocol Status** screen displays by default.

This screen displays LACP group aggregator ID, member port number(s) and the group status.

Figure 42 Link Aggregation Control Protocol Status

Index	Aggregator ID	Enabled Ports	Synchronized Ports
1	[(0000,00-00-00-00-00-00,0000,00,0000)] [(0000,00-00-00-00-00-00,0000,00,0000)]	-	-

Polling Interval(s)

The following table describes the labels in this screen.

Table 33 Link Aggregation Control Protocol Status

LABEL	DESCRIPTION
Index	This field displays the trunk ID to identify a trunk group, that is, one logical link containing multiple ports.
Aggregator ID	This field displays the link aggregation ID. Link aggregation ID consists of the following: system priority, MAC address, key, port priority and port number. Refer to Section 14.1.2 on page 114 for more information on this field.
Enabled Ports	These are the ports you have configured in the Link Aggregation screen to be in the trunk group.
Synchronized Ports	These are the ports that are currently transmitting data as one logical link in this trunk group.

1. Port Priority and Port Number are 0 as it is the aggregator ID for the trunk group, not the individual port.

Table 33 Link Aggregation Control Protocol Status (continued)

LABEL	DESCRIPTION
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking Set Interval .
Stop	Click Stop to halt statistic polling.

14.3 Link Aggregation Setup

Click **Configuration** in the **Link Aggregation Control Protocol Status** screen to display the screen shown next.

See [Section 14.1 on page 113](#) for background information.

Figure 43 Link Aggregation Control Protocol > Configuration

The screenshot shows the 'Link Aggregation Control Protocol' configuration interface. At the top, there's a header with 'Link Aggregation' and a 'Status' link. Below it, the 'Link Aggregation Control Protocol' section includes an 'Active' checkbox (unchecked) and a 'System Priority' text box containing '65535'. A horizontal separator follows. The next section has a table with columns 'Group ID', 'Active', and 'Dynamic(LACP)'. The 'Group ID' column contains 'T1', while 'Active' and 'Dynamic(LACP)' are checkboxes (both unchecked). Another horizontal separator is present. Below that is a table with columns 'Port', 'Group', and 'LACP Timeout'. It lists two ports: '17' and '18'. For each port, the 'Group' is set to 'None' (via a dropdown) and the 'LACP Timeout' is '30 seconds'. At the bottom, there are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 34 Link Aggregation Control Protocol > Configuration

LABEL	DESCRIPTION
Link Aggregation Control Protocol	
Active	Select this checkbox to enable Link Aggregation Control Protocol (LACP).
System Priority	LACP system priority is a number between 1 and 65,355. The switch with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP “server”. The LACP “server” controls the operation of LACP setup. Enter a number to set the priority of an active port using Link Aggregate Control Protocol (LACP). The smaller the number, the higher the priority level.
Group ID	The field identifies the link aggregation group, that is, one logical link containing multiple ports
Active	Select this option to activate a trunk group.
Dynamic (LACP)	Select this check box to enable LACP for a trunk.
Port	This field displays the port number.
Group	Select the trunk group to which a port belongs.

Table 34 Link Aggregation Control Protocol > Configuration (continued)

LABEL	DESCRIPTION
LACP Timeout	Timeout is the time interval between the individual port exchanges of LACP packets in order to check that the peer port in the trunk group is still up. If a port does not respond after three tries, then it is deemed to be “down” and is removed from the trunk. Set a short timeout (one second) for busy trunked links to ensure that disabled ports are removed from the trunk group as soon as possible. Select either 1 second or 30 seconds.
Apply	Click Apply to save your changes back to the switch.
Cancel	Click Cancel to begin configuring this screen afresh.

Port Authentication

This chapter describes the 802.1x authentication method and RADIUS server connection setup.

15.1 Port Authentication Overview

IEEE 802.1x is an extended authentication protocol² that allows support of RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.

15.1.1 RADIUS

RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS authentication allows you to validate an unlimited number of users from a central location.

Figure 44 RADIUS Server



15.2 Configure Port Authentication

To enable port authentication, first activate IEEE802.1x security (both on the switch and the port(s)) then configure the RADIUS server settings.

Click **Advanced Application > Port Authentication** in the navigation panel to display the screen as shown.

-
2. At the time of writing, only Windows XP of the Microsoft operating systems supports it. See the Microsoft web site for information on other Windows operating system support. For other operating systems, see its documentation. If your operating system does not support 802.1x, then you may need to install 802.1x client software.

Figure 45 Port Authentication

Port Authentication

RADIUS 802.1x [Click here](#) [Click here](#)

15.2.1 Activate IEEE 802.1x Security

From the **Port Authentication** screen, display the configuration screen as shown.

See [Section 15.1 on page 117](#) for background information.

Figure 46 Port Authentication > 802.1x

802.1x Port Authentication

Active ☐

Port	Active	Reauthentication	Reauthentication Timer
1	<input type="checkbox"/>	On	3600 seconds
2	<input type="checkbox"/>	On	3600 seconds
3	<input type="checkbox"/>	On	3600 seconds
15	<input type="checkbox"/>	On	3600 seconds
16	<input type="checkbox"/>	On	3600 seconds

Apply Cancel

The following table describes the labels in this screen.

Table 35 Port Authentication > 802.1x

LABEL	DESCRIPTION
Active	Select this check box to permit 802.1x authentication on the switch. Note: You must first enable 802.1x authentication on the switch before configuring it on each port.
Port	This field displays a port number.
Active	Select this checkbox to permit 802.1x authentication on this port. You must first allow 802.1x authentication on the switch before configuring it on each port.
Reauthentication	Specify if a subscriber has to periodically re-enter his or her username and password to stay connected to the port.
Reauthentication Timer	Specify how often a client has to re-enter his or her username and password to stay connected to the port. It is recommended that you enter a number more than 60 seconds. The valid range is between 1 and 65535 seconds.
Apply	Click Apply to save your changes back to the switch.
Cancel	Click Cancel to begin configuring this screen afresh.

15.2.2 Configuring RADIUS Server Settings

From the **Port Authentication** screen, click **RADIUS** to display the configuration screen as shown.

Use this screen to configure RADIUS server settings. See [Section 15.1 on page 117](#) for background information.

Figure 47 Port Authentication > RADIUS

The following table describes the labels in this screen.

Table 36 Port Authentication > RADIUS

LABEL	DESCRIPTION
Authentication Server	
IP Address	Enter the IP address of the external RADIUS server in dotted decimal notation.
UDP Port	The default port of the RADIUS server for authentication is 1812 . You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS server and the switch. This key is not sent over the network. This key must be the same on the external RADIUS server and the switch.
Apply	Click Apply to save your changes back to the switch.
Cancel	Click Cancel to begin configuring this screen afresh.

Port Security

This chapter shows you how to set up port security.

16.1 Port Security Overview

Port security allows only packets with dynamically learned MAC addresses and/or configured static MAC addresses to pass through a port on the switch. The switch can learn up to 16K MAC addresses in total with no limit on individual ports other than the sum cannot exceed 16K.

For maximum port security, enable this feature, disable MAC address learning and configure static MAC address(es) for a port. It is not recommended you disable **Port Security** together with MAC address learning as this will result in many broadcasts.

16.2 Port Security Setup

Click **Advanced Application > Port Security** in the navigation panel to display the screen as shown.

Figure 48 Port Security

Port	Active	Address Learning	Limited Number of Learned MAC Address
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
15	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
16	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
17	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
18	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0

Apply Cancel

The following table describes the labels in this screen.

Table 37 Port Security

LABEL	DESCRIPTION
Active	Select this check box to enable the port security feature on the switch.
Port	This field displays a port number.
Active	Select this check box to enable the port security feature on this port. The switch forwards packets whose MAC address(es) is in the MAC address table on this port. Packets with no matching MAC address(es) are dropped. Clear this check box to disable the port security feature. The switch forwards all packets on this port.
Address Learning	MAC address learning reduces outgoing broadcast traffic. For MAC address learning to occur on a port, the port itself must be active with address learning enabled.
Limited Number of Learned MAC Address	Use this field to limit the number of (dynamic) MAC addresses that may be learned on a port. For example, if you set this field to "5" on port 2, then only the devices with these five learned MAC addresses may access port 2 at any one time. A sixth device would have to wait until one of the five learned MAC addresses aged out. MAC address aging out time can be set in the Switch Setup screen. The valid range is from 0 to 16K. "0" means this feature is disabled, so the switch will learn MAC addresses up to the global limit of 16K.
Apply	Click Apply to save your changes back to the switch.
Cancel	Click Cancel to begin configuring this screen afresh.

Queuing Method

This chapter introduces the queuing methods supported.

17.1 Queuing Method Overview

Queuing is used to help solve performance degradation when there is network congestion. Use the **Queuing Method** screen to configure queuing algorithms for outgoing traffic. See also **Priority Queue Assignment in Switch Setup** and **802.1p Priority in Port Setup** for related information.

Queuing algorithms allow switches to maintain separate queues for packets from each individual source or flow and prevent a source from monopolizing the bandwidth.

The switch has eight physical queues, Q0 to Q7. Q7 has the highest priority and Q0 has the lowest.

Table 38 Physical Queue Priority

QUEUE	PRIORITY
Q7	8 (Highest)
Q6	7
Q5	6
Q4	5
Q3	4
Q2	3
Q1	2
Q0	1 (Lowest)

17.1.1 Strict Priority Queuing (SPQ)

Strict Priority Queuing (SPQ) services queues based on priority only. As traffic comes into the switch, traffic on the highest priority queue, Q3 is transmitted first. When that queue empties, traffic on the next highest-priority queue, Q2 is transmitted until Q2 empties, and then traffic is transmitted on Q1 and so on. If higher priority queues never empty, then traffic on lower priority queues never gets sent. SPQ does not automatically adapt to changing network requirements.

17.1.2 Weighted Fair Scheduling (WFS)

Weighted Fair Scheduling is used to guarantee each queue's minimum bandwidth based on their bandwidth weight (portion) (the number you configure in the **Weight** field) when there is traffic congestion. WFS is activated only when a port has more traffic than it can handle.

Queues with larger weights get more guaranteed bandwidth than queues with smaller weights. This queuing mechanism is highly efficient in that it divides any available bandwidth across the different traffic queues. By default, the weight for Q0 is 1, for Q1 is 2, for Q2 is 3, and so on. Guaranteed bandwidth is calculated as follows:

Guaranteed bandwidth = Queue Weight ÷ Total Queue Weight × Port Speed

For example, using the default setting, Q0 on Port 1 gets a guaranteed bandwidth of:

$$1 \div (1+2+3+4+5+6+7+8) \times 100 \text{ Mbps} = 3 \text{ Mbps}$$

17.2 Configuring Queuing

Click **Advanced Application > Queuing Method** in the navigation panel.

Figure 49 Queuing Method

Queuing Method

Method

☒ Strictly Priority
☐ Weighted Fair Scheduling

FE Port SPQ Enable: None

Port	Weight							
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
1	1	2	3	4	5	6	7	8
2	1	2	3	4	5	6	7	8
3	1	2	3	4	5	6	7	8
4	1	2	3	4	5	6	7	8
5	1	2	3	4	5	6	7	8
6	1	2	3	4	5	6	7	8
7	1	2	3	4	5	6	7	8
8	1	2	3	4	5	6	7	8
9	1	2	3	4	5	6	7	8
10	1	2	3	4	5	6	7	8
11	1	2	3	4	5	6	7	8
12	1	2	3	4	5	6	7	8
13	1	2	3	4	5	6	7	8
14	1	2	3	4	5	6	7	8
15	1	2	3	4	5	6	7	8
16	1	2	3	4	5	6	7	8
17	1	2	3	4	5	6	7	8
18	1	2	3	4	5	6	7	8

Apply Cancel

The following table describes the labels in this screen.

Table 39 Queuing Method

LABEL	DESCRIPTION
Method	<p>Select Strictly Priority or Weighted Fair Scheduling.</p> <p>Strictly Priority services queues based on priority only. When the highest priority queue empties, traffic on the next highest-priority queue begins. Q7 has the highest priority and Q0 the lowest.</p> <p>Weighted Fair Scheduling is used to guarantee each queue's minimum bandwidth based on their bandwidth portion (weight) (the number you configure in the Weight field). Queues with larger weights get more guaranteed bandwidth than queues with smaller weights.</p>
FE Port SPQ Enable	<p>This field is applicable only when you select Weighted Fair Scheduling.</p> <p>Select a queue (Q0 to Q7) to have the switch use Strictly Priority to service the subsequent queue(s) after and including the specified queue for the 10/100 Mbps Ethernet ports. For example, if you select Q5, the switch services traffic on Q5, Q6 and Q7 using Strictly Priority.</p> <p>Select None to always use Weighted Fair Scheduling for the 10/100 Mbps Ethernet ports.</p>
Port	This label shows the port you are configuring.
Weight Q0~Q7	<p>When you select Weighted Fair Scheduling, enter the queue weight here. Bandwidth is divided across the different traffic queues according to their weights. Queues with larger weights get more guaranteed bandwidth than queues with smaller weights.</p>
Apply	Click Apply to save your changes back to the switch.
Cancel	Click Cancel to begin configuring this screen afresh.

Classifier

This chapter introduces and shows you how to configure the packet classifier on the switch.

18.1 Classifier Overview

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

A layer-2 classifier groups traffic according to the Ethernet type, VLAN group, MAC address and/or port number. A layer-3 classifier groups traffic according to the IP address and/or TCP/UDP protocol number.

Configure QoS on the switch to group and prioritize application traffic and fine-tune network performance. Setting up QoS involves two separate steps:

- 1 Configure classifiers to sort traffic into different flows.
- 2 Configure policy rules to define actions to be performed for a classified traffic flow (refer to [Chapter 19 on page 133](#) to configure policy rules).

18.2 Configuring a Classifier

Use the **Classifier** screen to define the classifiers. After you define the classifier, you can specify actions (or policy) to act upon the traffic that match the rules. To configure policy rules, refer to [Chapter 19 on page 133](#).

Click **Advanced Application** and **Classifier** in the navigation panel to display the configuration screen as shown.

Figure 50 Classifier

Classifier

Active ☐

Name

Packet Format

VLAN ☒ Any ☐

Layer 2

Ethernet Type ☒ All ☐ Others (Hex)

Source

MAC Address ☒ Any ☐ MAC : : : : :

Port

Destination

MAC Address ☒ Any ☐ MAC : : : : :

Layer 3

DSCP ☒ Any ☐

IP Protocol ☒ All ☐ Establish Only ☐ Others (Dec)

Source

IP Address / Address Prefix /

Socket Number ☒ Any ☐

Destination

IP Address / Address Prefix /

Socket Number ☒ Any ☐

Add Cancel Clear

Index	Active	Name	Rule	Delete
1	Yes	Example	SrcMac = 00:50:ba:ad:4f:81; SrcPort = port 2;	<input type="checkbox"/>

Delete Cancel

The following table describes the related labels in this screen.

Table 40 Classifier

LABEL	DESCRIPTION
Active	Select this option to enable this rule.
Name	Type a descriptive name (up to 32 printable ASCII characters) for this rule. This is for identification purpose only.
Packet Format	Specify the format of the packet. Choices are All , 802.3 tagged , 802.3 untagged , Ethernet II tagged and Ethernet II untagged . A value of 802.3 indicates that the packets are formatted according to the IEEE 802.3 standards. A value of Ethernet II indicates that the packets are formatted according to RFC 894, Ethernet II encapsulation.
Layer 2	Specify the fields below to configure a layer-2 classifier.
VLAN	Select Any to classify traffic from any VLAN or select the second option and specify the source VLAN ID in the field provided.

Table 40 Classifier (continued)

LABEL	DESCRIPTION
Ethernet Type	Select an Ethernet type or select Other and enter the Ethernet type number in hexadecimal value. Refer to Table 41 on page 130 for information. Select All if you don't know.
Source	
MAC Address	Select Any to apply the rule to all MAC addresses. To specify a source, select MAC and type a MAC address in valid MAC address format (six hexadecimal character pairs).
Port	Select the port to which the rule should be applied. You may choose one port only or all ports (All Ports).
Destination	
MAC Address	Select Any to apply the rule to all MAC addresses. To specify a destination, select the second choice and type a MAC address in valid MAC address format (six hexadecimal character pairs).
Layer 3 Specify the fields below to configure a layer 3 classifier.	
DSCP	Select Any to classify traffic from any DSCP or select the second option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
IP Protocol	Select an IP protocol type or select Other and enter the protocol number in decimal value. Refer to Table 42 on page 130 for more information. You may select Establish Only for TCP protocol type. This means that the switch will pick out the packets that are sent to establish TCP connections.
Source	
IP Address/ Address Prefix	Enter a source IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask.
Socket Number	Note: You <i>must</i> select either UDP or TCP in the IP Protocol field before you configure the socket numbers. Select Any to apply the rule to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number.
Destination	
IP Address/ Address Prefix	Enter a destination IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask.
Socket Number	Note: You <i>must</i> select either UDP or TCP in the IP Protocol field before you configure the socket numbers. Select Any to apply the rule to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number.
Add	Click Add to save the changes.
Cancel	Click Cancel to reset the fields back to your previous configuration.
Clear	Click Clear to set the above fields back to the factory defaults.
Index	This field displays the index number of the rule. Click an index number to edit the rule.
Active	This field displays Yes when the rule is activated and No when is it deactivated.

Table 40 Classifier (continued)

LABEL	DESCRIPTION
Name	This field displays the descriptive name for this rule. This is for identification purpose only.
Rule	This field displays a summary of the classifier rule's settings.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

The following table shows some other common Ethernet types and the corresponding protocol number.

Table 41 Common Ethernet Type Number

Ethernet Type	number
IP ETHII	0800
X.75 Internet	0801
NBS Internet	0802
ECMA Internet	0803
Chaosnet	0804
X.25 Level 3	0805
XNS Compat	0807
Banyan Systems	0BAD
BBN Simnet	5208
IBM SNA	80D5
AppleTalk AARP	80F3

Some of the most common protocol port numbers are:

Table 42 Common Protocol Port Number

PORT NUMBER	NAME
21	FTP
23	Telnet
25	SMTP
53	DNS
80	HTTP
110	POP3

18.3 Classifier Example

The following screen shows an example where you configure a classifier that identifies all traffic from MAC address 00:50:ba:ad:4f:81 on port 2.

After you have configured a classifier, you can configure a policy (in the **Policy** screen) to define action(s) on the classified traffic flow.

Figure 51 Classifier Example

Classifier

Active ☒

Name

Packet Format

VLAN ☒ Any

Ethernet ☒ All ☐ Others (Hex)

Layer 2

Source MAC Address ☒ Any ☐ MAC : : : : :

Port

Destination MAC Address ☒ Any ☐ MAC : : : : :

DSCP ☒ Any

IP Protocol ☒ All ☐ Establish Only ☐ Others (Dec)

Layer 3

Source IP Address / Address Prefix /

Socket Number ☒ Any

Destination IP Address / Address Prefix /

Socket Number ☒ Any

Index	Active	Name	Rule	Delete
1	Yes	Example	SrcMac = 00:50:ba:ad:4f:81; SrcPort = port 2;	<input type="checkbox"/>

This chapter shows you how to configure policy rules.

19.1 Policy Overview

A classifier distinguishes traffic into flows based on the configured criteria (refer to [Chapter 18 on page 127](#) for more information). A policy rule ensures that a traffic flow gets the requested treatment in the network.

19.1.1 DiffServ

DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

19.1.2 DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different kinds of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

19.2 Configuring a Policy



You must first configure a classifier in the **Classifier** screen. Refer to [Chapter 18 on page 127](#) for more information.

Click **Advanced Application** and then **Policy Rule** in the navigation panel to display the screen as shown.

Figure 52 Policy

Policy

Active☐

Name

Classifier(s)

Example

Parameters

General

VLAN ID

EgressPort

Port1

Outgoing packet format for Egress port

☒ Tag ☐ Untag

Priority

0

DSCP

TOS

0

Metering

Bandwidth Mbps

Out-of-Profile DSCP

Action

Forwarding

☒ No change

☐ Discard the packet

☐ Do not drop the matching frame previously marked for dropping

Priority

☒ No change

☐ Set the packet's 802.1 priority

☐ Send the packet to priority queue

☐ Replace the 802.1 priority field with the IP TOS value

Diffserv

☒ No change

☐ Set the packet's TOS field

☐ Replace the IP TOS field with the 802.1 priority value

☐ Set the Diffserv Codepoint field in the frame

Outgoing

☐ Send the packet to the mirror port

☐ Send the packet to the egress port

☐ Send the matching frames(broadcast or DLF, multicast, marked for dropping or to be sent to the CPU) to the egress port

☐ Set the packet's VLAN ID

Metering

☐ Enable

Out-of-profile action

☐ Drop the packet

☐ Change the DSCP value

☐ Do not drop the matching frame previously marked for dropping

Add

Cancel

Clear

Index	Active	Name	Classifier(s)	Delete
1	Yes	Test	Example;	<input type="checkbox"/>

Delete

Cancel

The following table describes the labels in this screen.

Table 43 Policy

LABEL	DESCRIPTION
Active	Select this option to enable the policy.
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Classifier(s)	This field displays the active classifier(s) you configure in the Classifier screen (refer to Chapter 18 on page 127). Select the classifier(s) to which this policy rule applies. To select more than one classifier, press [SHIFT] and select the choices at the same time.
Parameters Set the fields below for this policy. You only have to set the field(s) that is related to the action(s) you configure in the Action field.	
General	
VLAN ID	Specify a VLAN ID number.
Egress Port	Select an outgoing port.
Outgoing packet format for Egress Port	Select Tag to add the specified VID to packets on the specified outgoing port. Otherwise, select Untag . The switch removes the VLAN tag from the packets.
Priority	Specify a priority level.
DSCP	Specify a DSCP (DiffServ Code Point) number between 0 and 63.
TOS	Specify the type of service (TOS) priority level.
Metering	You can configure the desired bandwidth available to a traffic flow. Traffic that exceeds the maximum bandwidth allocated (in cases where the network is congested) is called out-of-profile traffic.
Bandwidth	Specify the bandwidth in mega bits per second (Mbps). Enter a number between 1 and 1023.
Out-of-Profile DSCP	Specify a new DSCP number (between 0 and 63) if you want to replace or remark the DSCP number for out-of-profile traffic.
Action Specify the action(s) the switch takes on the associated classified traffic flow.	
Forwarding	Select No change to forward the packets. Select Discard packet to drop the packets. Select Do not drop the matching frame previously marked for dropping to retain the frames that were marked to be dropped before.
Priority	Select No change to keep the priority setting of the frames. Select Set the packet's 802.1 priority to replace the 802.1 priority field with the value you set in the Priority field. Select Send the packet to priority queue to put the packets in the designated queue. Select Replace the 802.1 priority field with IP TOS value to replace the 802.1 priority field with the value you set in the TOS field.
DiffServ	Select No change to keep the TOS and/or DSCP fields in the packets. Select Set the packet's TOS field to set the TOS field with the value you configure in the TOS field. Select Replace the IP TOS field with the 802.1 priority value to replace the TOS field with the value you configure in the Priority field. Select Set the Diffserv Codepoint field in the frame to set the DSCP field with the value you configure in the DSCP field.

Table 43 Policy (continued)

LABEL	DESCRIPTION
Outgoing	Select Send the packet to the mirror port to send the packet to the mirror port. Select Send the packet to the egress port to send the packet to the egress port. Select Send the matching frames (broadcast or DLF, multicast, marked for dropping or to be sent to the CPU) to the egress port to send the broadcast, multicast, DLF, marked-to-drop or CPU frames to the egress port. Select Set the packet's VLANID to set the VLAN ID of the packet with the value you configure in the VLANID field.
Metering	Select Enable to activate bandwidth limitation on the traffic flow(s) then set the actions to be taken on out-of-profile packets.
Out-of-profile Action	Select the action(s) to be performed for out-of-profile traffic. Select Drop the packet to discard the out-of-profile traffic. Select Change the DSCP Value to replace the DSCP field with the value specified in the Out-of-Profile DSCP field above. Select Do not drop the matching frame previously marked for dropping to queue the frames that are marked to be dropped.
Add	Click Add to inset the entry to the summary table below.
Cancel	Click Cancel to reset the fields back to your previous configuration.
Clear	Click Clear to set the above fields back to the factory defaults.
Index	This field displays the policy index number. Click an index number to edit the policy.
Active	This field displays Yes when policy is activated and No when is it deactivated.
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Classifier(s)	This field displays the name(s) of the classifier to which this policy applies.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

19.3 Policy Example

The figure below shows an example **Policy** screen where you configure a policy to limit bandwidth and discard out-of-profile traffic on a traffic flow classified using the **Example** classifier (refer to [Section 18.3 on page 130](#)).

Figure 53 Policy Example

Policy

Active ☒

Name

Classifier(s)

Parameters

VLAN ID	<input type="text" value="1"/>	General	Bandwidth	<input type="text" value="1000"/> Mbps
EgressPort	<input type="text" value="Port1"/>		Out-of-Profile DSCP	<input type="text" value="63"/>
Outgoing packet format for Egress port	<input checked="" type="radio"/> Tag <input type="radio"/> Untag			
Priority	<input type="text" value="0"/>			
DSCP	<input type="text"/>			
TOS	<input type="text" value="0"/>			

Action

Forwarding

☒ No change

☐ Discard the packet

☐ Do not drop the matching frame previously marked for dropping

Priority

☒ No change

☐ Set the packet's 802.1 priority

☐ Send the packet to priority queue

☐ Replace the 802.1 priority field with the IP TOS value

Diffserv

☒ No change

☐ Set the packet's TOS field

☐ Replace the IP TOS field with the 802.1 priority value

☐ Set the Diffserv Codepoint field in the frame

Outgoing

☐ Send the packet to the mirror port

☐ Send the packet to the egress port

☐ Send the matching frames(broadcast or DLF, multicast, marked for dropping or to be sent to the CPU) to the egress port

☐ Set the packet's VLAN ID

Metering

☐ Enable

Out-of-profile action

☒ Drop the packet

☐ Change the DSCP value

☐ Do not drop the matching frame previously marked for dropping

VLAN Stacking

This chapter shows you how to configure VLAN stacking on your switch. See the chapter on VLANs for more background information on Virtual LAN

20.1 VLAN Stacking Overview

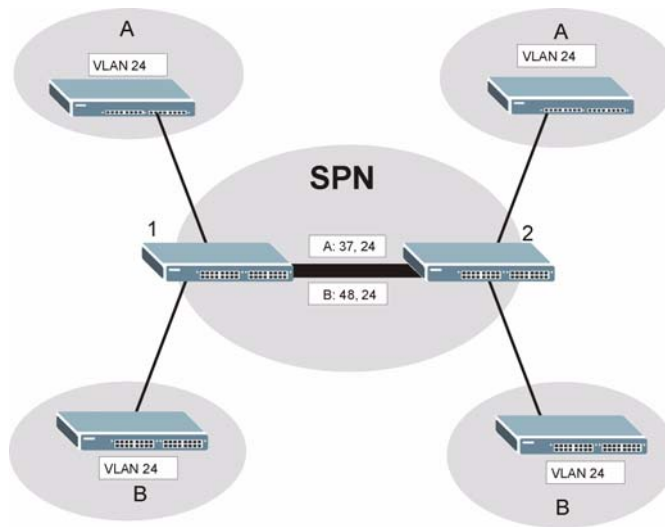
A service provider can use VLAN stacking to allow it to distinguish multiple customers VLANs, even those with the same (customer-assigned) VLAN ID, within its network.

Use VLAN stacking to add an outer VLAN tag to the inner IEEE 802.1Q tagged frames that enter the network. By tagging the tagged frames (“double-tagged” frames), the service provider can manage up to 4,094 VLAN groups with each group containing up to 4,094 customer VLANs. This allows a service provider to provide different service, based on specific VLANs, for many different customers.

A service provider’s customers may require a range of VLANs to handle multiple applications. A service provider’s customers can assign their own inner VLAN tags on ports for these applications. The service provider can assign an outer VLAN tag for each customer. Therefore, there is no VLAN tag overlap among customers, so traffic from different customers is kept separate.

20.1.1 VLAN Stacking Example

In the following example figure, both **A** and **B** are Service Provider’s Network (SPN) customers with VPN tunnels between their head offices and branch offices respectively. Both have an identical VLAN tag for their VLAN group. The service provider can separate these two VLANs within its network by adding tag **37** to distinguish customer **A** and tag **48** to distinguish customer **B** at edge device **1** and then stripping those tags at edge device **2** as the data frames leave the network.

Figure 54 VLAN Stacking Example

20.2 VLAN Stacking Port Roles

Each port can have three VLAN stacking “roles”, **Normal**, **Access Port** and **Tunnel Port** (the latter is for Gigabit ports only).

- Select **Normal** for “regular” (non-VLAN stacking) IEEE 802.1Q frame switching.
- Select **Access Port** for ingress ports on the service provider's edge devices (1 and 2 in the VLAN stacking example figure). The incoming frame is treated as "untagged", so a second VLAN tag (outer VLAN tag) can be added.



Static VLAN Tx Tagging MUST be disabled on a port where you choose **Normal** or **Access Port**.

- Select **Tunnel Port** (available for Gigabit ports only) for egress ports at the edge of the service provider's network. All VLANs belonging to a customer can be aggregated into a single service provider's VLAN (using the outer VLAN tag defined by SP VID).



Static VLAN Tx Tagging MUST be enabled on a port where you choose **Tunnel**.

20.3 VLAN Tag Format

A VLAN tag (service provider VLAN stacking or customer IEEE 802.1Q) consists of the following three fields.

Table 44 VLAN Tag Format

Type	Priority	VID
------	----------	-----

Type is a standard Ethernet type code identifying the frame and indicates that whether the frame carries IEEE 802.1Q tag information. **SP TPID** (Service Provider Tag Protocol Identifier) is the service provider VLAN stacking tag type. Many vendors use 0x8100 or 0x9100.

TPID (Tag Protocol Identifier) is the customer IEEE 802.1Q tag.

- If the VLAN stacking port role is **Access Port**, then the switch adds the **SP TPID** tag to all incoming frames on the service provider's edge devices (1 and 2 in the VLAN stacking example figure).
- If the VLAN stacking port role is **Tunnel Port**, then the switch only adds the **SP TPID** tag to all incoming frames on the service provider's edge devices (1 and 2 in the VLAN stacking example figure) that have an **SP TPID** different to the one configured on the switch. (If an incoming frame's **SP TPID** is the same as the one configured on the switch, then the switch will not add the tag.)

Priority refers to the IEEE 802.1p standard that allows the service provider to prioritize traffic based on the class of service (CoS) the customer has paid for.

- On the switch, configure priority level of inner IEEE 802.1Q tag in the **Port Setup** screen.
- "0" is the lowest priority level and "7" is the highest.

VID is the VLAN ID. **SP VID** is the VID for the second (service provider's) VLAN tag.

20.3.1 Frame Format

The frame format for an untagged Ethernet frame, a single-tagged 802.1Q frame (customer) and a "double-tagged" 802.1Q frame (service provider) is shown next.

Configure the fields as circled in the switch **VLAN Stacking** screen.

Table 45 Single and Double Tagged 802.11Q Frame Format

						DA	SA	Len/Etype	Data	FCS	Untagged Ethernet frame
			DA	SA	TPID	Priority	VID	Len/Etype	Data	FCS	IEEE 802.1Q customer tagged frame
DA	SA	SPTPID	Priority	VID	TPID	Priority	VID	Len/Etype	Data	FCS	Double-tagged frame

Table 46 IEEE 802.1Q Frame

DA	Destination Address	Priority	802.1p Priority
SA	Source Address	Len/Etype	Length and type of Ethernet frame

Table 46 IEEE 802.1Q Frame

(SP)TPID	(Service Provider) Tag Protocol Identifier	Data	Frame data
VID	VLAN ID	FCS	Frame Check Sequence

20.4 Configuring VLAN Stacking

Click **Advanced Application** and then **VLAN Stacking** in the navigation panel to display the screen as shown.

Figure 55 VLAN Stacking

The following table describes the labels in this screen.

Table 47 VLAN Stacking

LABEL	DESCRIPTION
Active	Select this checkbox to enable VLAN stacking on the switch.
SP TPID	SP TPID is a standard Ethernet type code identifying the frame and indicates whether the frame carries IEEE 802.1Q tag information. Choose 0x8100 or 0x9100 from the drop-down list box or select Others and then enter a four-digit hexadecimal number from 0x0000 to 0xFFFF. 0x denotes a hexadecimal number. It does not have to be typed in the Others text field.
Port	The port number identifies the port you are configuring.
Role	<p>Select Normal to have the switch ignore frames received (or transmitted) on this port with VLAN stacking tags. Anything you configure in SPVID and Priority are ignored.</p> <p>Select Access Port to have the switch add the SP TPID tag to all incoming frames received on this port. Select Access Port for ingress ports at the edge of the service provider's network.</p> <p>Select Tunnel Port (available for Gigabit ports only) for egress ports at the edge of the service provider's network.</p> <p>In order to support VLAN stacking on a port, the port must be able to allow frames of 1526 Bytes (1522 Bytes + 4 Bytes for the second tag) to pass through it.</p>
SPVID	SPVID is the service provider's VLAN ID (the outer VLAN tag). Enter the service provider ID (from 1 to 4094) for frames received on this port. See Chapter 7 on page 87 for more background information on VLAN ID.

Table 47 VLAN Stacking (continued)

LABEL	DESCRIPTION
Priority	Select a number from the drop-down list box to configure the priority level of the outer tag. "0" is the lowest priority level and "7" is the highest. Note: Configure the priority level of the inner IEEE 802.1Q tag in the Port Setup screen.
Apply	Click Apply to save your changes back to the switch.
Cancel	Click Cancel to begin configuring this screen afresh.

Multicast

This chapter shows you how to configure various multicast features.

21.1 Multicast Overview

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender to 1 recipient) or Broadcast (1 sender to everybody on the network). Multicast delivers IP packets to just a group of hosts on the network.

IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a multicast group - it is not used to carry user data. Refer to RFC 1112 and RFC 2236 for information on IGMP versions 1 and 2 respectively.

See [Section 21.3 on page 146](#) to configure multicast.

21.1.1 IP Multicast Addresses

In IPv4, a multicast address allows a device to send packets to a specific group of hosts (multicast group) in a different subnetwork. A multicast IP address represents a traffic receiving group, not individual receiving devices. IP addresses in the Class D range (224.0.0.0 to 239.255.255.255) are used for IP multicasting. Certain IP multicast numbers are reserved by IANA for special purposes (see the IANA web site for more information).

21.1.2 IGMP Filtering

With IGMP filtering, you can control which IGMP groups a subscriber on a port can join. This allows you to control the distribution of multicast services (such as content information distribution) based on service plans and types of subscription.

You can set the switch to filter the multicast group join reports on a per-port basis by configuring an IGMP filtering profile and associating the profile to a port.

21.1.3 IGMP Snooping

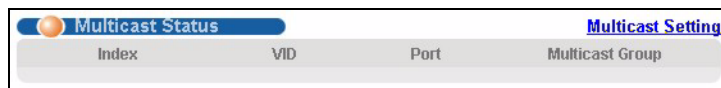
A layer-2 switch can passively snoop on IGMP Query, Report and Leave (IGMP version 2) packets transferred between IP multicast routers/switches and IP multicast hosts to learn the IP multicast group membership. It checks IGMP packets passing through it, picks out the group registration information, and configures multicasting accordingly.

Without IGMP snooping, multicast traffic is treated in the same manner as broadcast traffic, you can configure the switch to forward or discard unknown multicast group traffic. With IGMP snooping, group multicast traffic is only forwarded to ports that are members of that group. IGMP snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your switch.

21.2 Multicast Status

Click **Advanced Application > Multicast** to display the screen as shown. This screen shows the multicast group information. Refer to [Section 21.1 on page 145](#) for more information on multicast.

Figure 56 Multicast Status .



Index	VID	Port	Multicast Group
-------	-----	------	-----------------

The following table describes the labels in this screen.

Table 48 Multicast Status

LABEL	DESCRIPTION
Index	This is the index number of the entry.
VID	This field displays the multicast VLAN ID.
Port	This field displays the port number that belongs to the multicast group.
Multicast Group	This field displays IP multicast group addresses.

21.3 Multicast Setup

Click **Advanced Application > Multicast** to display the screen as shown. Use this screen to enable and configure multicast settings on the switch and apply IGMP profiles to ports.

See [Section 21.1 on page 145](#) for background information.

Figure 57 Multicast

Port	Immed. Leave	Group Limited	Max Group Num.	IGMP Filtering Profile	IGMP Querier Mode
1	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto
2	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto
3	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto
4	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto
5	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto
6	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto
7	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto
8	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto
9	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto
10	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto
11	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto
12	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto
13	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto
14	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto
15	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto
16	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto
17	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto
18	<input type="checkbox"/>	<input type="checkbox"/>	0	Default	Auto

The following table describes the labels in this screen.

Table 49 Multicast

LABEL	DESCRIPTION
IGMP Snooping	
Active	Select Active to enable IGMP snooping to forward group multicast traffic only to ports that are members of that group
Host Timeout	Specify the time (from 1 to 16,716,450) in seconds that elapses before the switch removes an IGMP group membership entry if it does not receive report messages from the host.
Leave Timeout	Enter an IGMP leave timeout value (from 1 to 16,716,450) in seconds. This defines how many seconds the switch waits before removing an IGMP snooping membership entry when an IGMP leave message is received from a host.
802.1p Priority	Select a priority level (0-7) to which the switch changes the priority in outgoing IGMP control packets. Otherwise, select No-Change to not replace the priority.
IGMP Filtering	Select Active to enable IGMP filtering to limit the IGMP groups a subscriber on a port can join.
Unknown Multicast Frame	Specify the action to perform when the switch receives an unknown multicast frame. Select Drop to discard the frame(s). Select Flooding to send the frame(s) to the destination device.
Port	This field displays the port number.
Immed. Leave	Select this option to set the switch to remove this port from the multicast tree when an IGMP version 2 leave message is received on this port. Select this option if there is only one host connected to this port.
Group Limited	Select this option to limit the number of multicast groups this port is allowed to join.
Max Group Num.	Select this option and enter a number to limit the number of multicast groups this port is allowed to join. Once a port is registered in the specified number of multicast groups, any new IGMP join report frame(s) is dropped on this port.
IGMP Filtering Profile	Select the name of the IGMP filtering profile to use for this port.

Table 49 Multicast (continued)

LABEL	DESCRIPTION
IGMP Querier Mode	<p>This field is applicable on the Ethernet ports.</p> <p>The switch treats an IGMP query port as being connected to an IGMP multicast router (or server). The switch forwards IGMP join or leave packets to an IGMP query port.</p> <p>Select Auto to have the switch use the port as an IGMP query port if the port receives IGMP query packets.</p> <p>Select Fixed to have the switch always use the port as an IGMP query port. Select this when you connect an IGMP multicast server to the port.</p> <p>Select Edge to stop the switch from using the port as an IGMP query port. The switch will not keep any record of an IGMP router being connected to this port. The switch does not forward IGMP join or leave packets to this port.</p>
Apply	Click Apply to save your changes back to the switch.
Cancel	Click Cancel to begin configuring this screen afresh.

21.4 IGMP Filtering Profile

IGMP filter profiles allow you to control access to IGMP multicast groups. This allows you to have a service available to a specific IGMP multicast group. You can configure an IGMP filter profile for an IGMP multicast group that has access to a service (like a SIP server for example). Within a profile, configure an IGMP filter to specify the multicast IP address ranges. Then assign the IGMP filter profile to the ports (in the **Multicast** screen) that are allowed to use the service.

Click **Advanced Application** and **Multicast** in the navigation panel. Click the **IGMP Filtering Profile** link to display the screen as shown.

Figure 58 Multicast > IGMP Filtering Profile

IGMP Filtering Profile Multicast Setting

Profile Setup

Profile Name	Start Address	End Address
<input type="text"/>	<input type="text" value="224.0.0.0"/>	<input type="text" value="224.0.0.0"/>

Profile Name	Start Address	End Address	Delete Profile	Delete Rule
Default	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="checkbox"/>	<input type="checkbox"/>

The following table describes the labels in this screen.

Table 50 Multicast > IGMP Filtering Profile

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile for identification purposes. To configure additional rule(s) for a profile that you have already added, enter the profile name and specify a different IP multicast address range.
Start Address	Type the starting multicast IP address for a range of multicast IP addresses that you want to belong to the IGMP filter profile.
End Address	Type the ending multicast IP address for a range of IP addresses that you want to belong to the IGMP filter profile. If you want to add a single multicast IP address, enter it in both the Start Address and End Address fields.
Add	Click Add to save the settings to the switch.
Clear	Click Clear to clear the fields to the factory defaults.
Profile Name	This field displays the descriptive name of the profile.
Start Address	This field displays the start of the multicast address range.
End Address	This field displays the end of the multicast address range.
Delete	To delete the profile(s) and all the accompanying rules, select the profile(s) that you want to remove in the Delete Profile column, then click the Delete button. To delete a rule(s) from a profile, select the rule(s) that you want to remove in the Delete Rule column, then click the Delete button.
Cancel	Click Cancel to clear the Delete Profile/Delete Rule check boxes.

21.5 MVR Overview

Multicast VLAN Registration is designed for applications (such as Media-on-Demand (MoD)) that use multicast traffic across a service provider network.

MVR allows one single multicast VLAN to be shared among different subscriber VLANs on the network. While isolated in different subscriber VLANs, connected devices can subscribe to and unsubscribe from the multicast stream in the multicast VLAN. This improves bandwidth utilization with reduced multicast traffic in the subscriber VLANs and simplifies multicast group management.

You must enable IGMP snooping to use MVR. However, MVR only responds to IGMP join and leave control messages from multicast groups that are configured under MVR. Join and leave reports from other multicast groups are managed by IGMP snooping.

The following figure shows a network example. The subscriber VLAN (**1, 2 and 3**) information is hidden from the streaming media server, **S**. In addition, the multicast VLAN information is only visible to the switch and **S**.

Figure 59 MVR Network Example



21.5.1 Types of MVR Ports

In MVR, a source port is a port on the switch that can send and receive multicast traffic in a multicast VLAN while a receiver port can only receive multicast traffic. Once configured, the switch maintains a forwarding table that matches the multicast stream to the associated multicast group.

21.5.2 MVR Modes

You can set your switch to operate in either dynamic or compatible mode.

In dynamic mode, the switch sends IGMP leave and join reports to the other multicast devices (such as multicast routers or servers) in the multicast VLAN. This allows the multicast devices to update the multicast forwarding table to forward or not forward multicast traffic to the receiver ports.

In compatible mode, the switch does not send any IGMP reports. In this case, you must manually configure the forwarding settings on the multicast devices in the multicast VLAN.

21.5.3 How MVR Works

The following figure shows a multicast television example where a subscriber device (such as a computer) in VLAN 1 receives multicast traffic from the streaming media server, S, via the switch. Multiple subscriber devices can connect through a port configured as the receiver on the switch.

When the subscriber selects a television channel, computer A sends an IGMP report to the switch to join the appropriate multicast group. If the IGMP report matches one of the configured MVR multicast group addresses on the switch, an entry is created in the forwarding table on the switch. This maps the subscriber VLAN to the list of forwarding destinations for the specified multicast traffic.

When the subscriber changes the channel or turns off the computer, an IGMP leave message is sent to the switch to leave the multicast group. The switch sends a query to VLAN 1 on the receiver port (in this case, a DSL port on the switch). If there is another subscriber device connected to this port in the same subscriber VLAN, the receiving port will still be on the list of forwarding destination for the multicast traffic. Otherwise, the switch removes the receiver port from the forwarding table.

Figure 60 MVR Multicast Television Example



21.6 General MVR Configuration

Use the **MVR** screen to create multicast VLANs and select the receiver port(s) and a source port for each multicast VLAN. Click **Advanced Application** and **Multicast** in the navigation panel. Click the **Multicast Setting** link and then the **MVR** link to display the screen as shown next.

See [Section 21.5 on page 149](#) for background information.



You can create up to three multicast VLANs and up to 266 multicast rules on the switch.



Your switch automatically creates a static VLAN (with the same VID) when you create a multicast VLAN in this screen.

Figure 61 MVR

MVR

Multicast SettingGroup Configuration

Active☐

Name

Multicast VLAN ID

802.1p Priority

0

Mode

☒ Dynamic☐ Compatible

Port	Source Port	Receiver Port	None	Tagging
1	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
2	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
3	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
15	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
16	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
17	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
18	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>

AddCancel

VLAN	Active	Name	Mode	Source Port	Receiver Port	802.1p	Delete
------	--------	------	------	-------------	---------------	--------	--------

DeleteCancel

The following table describes the related labels in this screen.

Table 51 MVR

LABEL	DESCRIPTION
Active	Select this check box to enable MVR to allow one single multicast VLAN to be shared among different subscriber VLANs on the network.
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Multicast VLAN ID	Enter the VLAN ID (1 to 4094) of the multicast VLAN.
802.1p Priority	Select a priority level (0-7) with which the switch replaces the priority in outgoing IGMP control packets (belonging to this multicast VLAN).
Mode	Specify the MVR mode on the switch. Choices are Dynamic and Compatible . Select Dynamic to send IGMP reports to all MVR source ports in the multicast VLAN. Select Compatible to set the switch not to send IGMP reports.
Port	This field displays the port number on the switch.
Source Port	This field is applicable for Ethernet ports. Select this option to set this port as the MVR source port that sends and receives multicast traffic.
Receiver Port	Select this option to set this port as a receiver port that only receives multicast traffic.
None	Select this option to set the port not to participate in MVR. No MVR multicast traffic is sent or received on this port.
Tagging	Select this checkbox if you want the port to tag the VLAN ID in all outgoing frames transmitted.
Add	Click Add to save the settings.
Cancel	Click Cancel to discard all changes.
VLAN	This field displays the multicast VLAN ID.
Active	This field displays whether the multicast group is enabled or not.
Name	This field displays the descriptive name for this setting.
Mode	This field displays the MVR mode.
Source Port	This field displays the source port number(s).
Receiver Port	This field displays the receiver port number(s).
802.1p	This field displays the priority with which the switch replaces the priority in outgoing IGMP control packets (belonging to this multicast VLAN).
Delete	To delete the group(s) and all the accompanying rules, select the group(s) that you want to remove in the Delete column, then click the Delete button.
Cancel	Click Cancel to clear the Delete check boxes.

21.7 MVR Group Configuration

All source ports and receiver ports belonging to a multicast group can receive multicast data sent to this multicast group.

See [Section 21.5 on page 149](#) for background information.

Configure MVR IP multicast group address(es) in the **Group Configuration** screen. Click **Group Configuration** in the **MVR** screen.



A port can belong to more than one multicast VLAN. However, IP multicast group addresses in different multicast VLANs cannot overlap.

Figure 62 MVR > Group Configuration

The following table describes the labels in this screen.

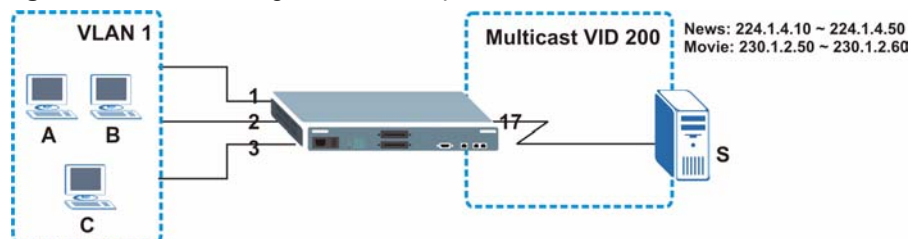
Table 52 MVR > Group Configuration

LABEL	DESCRIPTION
Multicast VLAN ID	Select a multicast VLAN ID (that you configured in the MVR screen) from the drop-down list box.
Name	Enter a descriptive name for identification purposes.
Start Address	Enter the starting IP multicast address of the multicast group in dotted decimal notation. Refer to Section 21.1.1 on page 145 for more information on IP multicast addresses.
End Address	Enter the ending IP multicast address of the multicast group in dotted decimal notation. Enter the same IP address as the Start Address field if you want to configure only one IP address for a multicast group. Refer to Section 21.1.1 on page 145 for more information on IP multicast addresses.
Add	Click Add to save the settings.
Cancel	Click Cancel to discard all changes.
MVLAN	This field displays the multicast VLAN ID.
Name	This field displays the descriptive name for this setting.
Start Address	This field displays the starting IP address of the multicast group.
End Address	This field displays the ending IP address of the multicast group.
Delete	Select Delete All and click Delete to remove all entries from the table. Select Delete Group and click Delete to remove the selected entry(ies) from the table.
Cancel	Select Cancel to clear the checkbox(es) in the table.

21.7.1 MVR Configuration Example

The following figure shows a network example where ports 1, 2 and 3 on the switch belong to VLAN 1. In addition, port 17 belongs to the multicast group with VID 200 to receive multicast traffic (the **News** and **Movie** channels) from the remote streaming media server, S. Computers A, B and C in VLAN are able to receive the traffic.

Figure 63 MVR Configuration Example



To configure the MVR settings on the switch, create a multicast group in the **MVR** screen and set the receiver and source ports.

Figure 64 MVR Configuration Example

Port	Source Port	Receiver Port	None	Tagging
1	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
2	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
3	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
4	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
5	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
6	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
7	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
8	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
9	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
10	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
11	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
12	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
13	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
14	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
15	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
16	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
17	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
18	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>

To set the switch to forward the multicast group traffic to the subscribers, configure multicast group settings in the **Group Configuration** screen. The following figure shows an example where two multicast groups (**News** and **Movie**) are configured for the multicast VLAN 200.

Figure 65 MVR Group Configuration Example

Group Configuration

MVR

Multicast VLAN ID

200

Name	Start Address	End Address
Movie	230.1.2.50	230.1.2.60

Add

Cancel

MVLAN	Name	Start Address	End Address	Delete All	Delete Group
200				<input type="checkbox"/>	
	News	224.1.4.10	224.1.4.50		<input type="checkbox"/>

Delete

Cancel

Differentiated Services

This chapter shows you how to configure Differentiated Services (DiffServ) on the switch.

22.1 DiffServ Overview

Quality of Service (QoS) is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

22.1.1 DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (ToS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

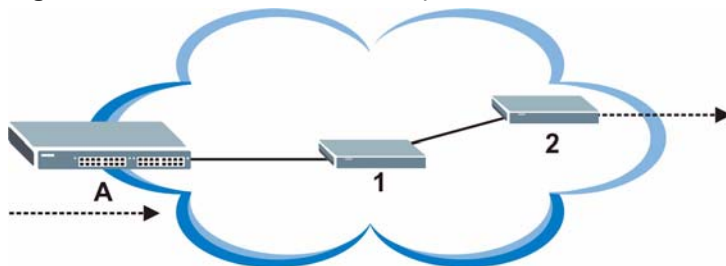
Figure 66 DiffServ: Differentiated Service Field

DSCP (6 bits)	DS (2 bits)
---------------	-------------

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule different kinds of traffic can be marked for different priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

22.1.2 DiffServ Network Example

The following figure depicts a simple DiffServ network consisting of a group of contiguous DiffServ-compliant network devices.

Figure 67 DiffServ Network Example

Switch **A** marks traffic flowing into the network based on the configured marking rules. Intermediary network devices **1** and **2** allocate network resources (such as bandwidth) by mapping the DSCP values and the associated policies.

22.2 Activating DiffServ

Activate DiffServ to allow the switch to enable DiffServ and apply marking rules and IEEE802.1p priority mapping on the selected port(s).

Click **Advanced Application > DiffServ** in the navigation panel to display the screen as shown.

Figure 68 DiffServ

Port	Active
1	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>
3	<input checked="" type="checkbox"/>
15	<input checked="" type="checkbox"/>
16	<input checked="" type="checkbox"/>
17	<input checked="" type="checkbox"/>
18	<input checked="" type="checkbox"/>

The following table describes the labels in this screen.

Table 53 DiffServ

LABEL	DESCRIPTION
Active	Select this option to enable DiffServ on the switch.
Default DSCP	Enter the default DSCP value (between 0 to 63) to use if no marking rule is configured for a traffic type.
Port	This field displays the index number of a port on the switch.
Active	Select this option to apply the default DSCP value you set in the Default DSCP field on a port.
Apply	Click Apply to save the changes.
Cancel	Click Cancel to start configuring this screen again.

22.3 DSCP-to-IEEE802.1p Priority Setting

You can configure the DSCP (DiffServ Code Point) to IEEE802.1p mapping to allow the switch to prioritize all traffic based on the incoming DSCP value according to the DiffServ-to-IEEE802.1p mapping table.

The following table shows the default DSCP-to-IEEE802.1P mapping.

Table 54 Default DSCP-IEEE802.1p Mapping

DSCP VALUE	0 – 7	8 – 15	16 – 23	24 – 31	32 – 39	40 – 47	48 – 55	56 – 63
IEEE802.1P	0	1	2	3	4	5	6	7

22.3.1 Configuring DSCP Setting

To change the DSCP-IEEE 802.1p mapping click the **DSCP Setting** link in the **DiffServ** screen to display the screen as shown next.

Figure 69 DiffServ > DSCP Setting

DSCP Setting		DSCP to 802.1p Mapping	
0	0	1	0
8	1	9	1
16	2	17	2
24	3	25	3
32	4	33	4
40	5	41	5
48	6	49	6
56	7	57	7

Apply Cancel

The following table describes the labels in this screen.

Table 55 DiffServ > DSCP Setting

LABEL	DESCRIPTION
0 ... 63	This is the DSCP classification identification number. To set the IEEE802.1p priority mapping, select the priority level from the drop-down list box.
Apply	Click Apply to save the changes.
Cancel	Click Cancel to discard all changes and start configuring the screen again.

PART IV

Routing Protocol

Static Route (163)

DHCP Relay (165)

Static Route

This chapter shows you how to configure static routes.

23.1 Configuring Static Route

Static routes tell the switch how to forward IP traffic when you configure the TCP/IP parameters manually.

Click **Routing Protocol > Static Routing** in the navigation panel to display the screen as shown.

Figure 70 Static Routing

Index	Active	Name	Destination Address	Subnet Mask	Gateway Address	Metric	Delete
1	Yes	Example	172.21.1.1	255.255.0.0	192.168.1.2	2	<input type="checkbox"/>

The following table describes the related labels you use to create a static route.

Table 56 Static Routing

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route.
Name	Enter a descriptive name for this route. This is for identification purpose only.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the subnet mask for this destination.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your switch that will forward the packet to the destination. The gateway must be a router on the same segment as your switch.

Table 56 Static Routing (continued)

LABEL	DESCRIPTION
Metric	The metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Add	Click Add to insert a new static route.
Cancel	Click Cancel to reset the above fields to your previous configuration.
Clear	Click Clear to set the above fields back to the factory defaults.
Index	This field displays the index number of the route. Click a number to edit the static route entry.
Active	This field displays Yes when the static route is activated and NO when it is deactivated.
Name	This field displays the descriptive name for this route. This is for identification purpose only.
Destination Address	This field displays the IP network address of the final destination.
Subnet Mask	This field displays the subnet mask for this destination.
Gateway Address	This field displays the IP address of the gateway. The gateway is an immediate neighbor of your switch that will forward the packet to the destination.
Metric	This field displays the cost of transmission for routing purposes.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

DHCP Relay

This chapter shows you how to configure the DHCP feature.

24.1 DHCP Overview

DHCP (Dynamic Host Configuration Protocol RFC 2131 and RFC 2132) allows individual computers to obtain TCP/IP configuration at start-up from a server. You can configure the switch to relay client DHCP requests to a DHCP server and the server's responses back to the clients.

24.1.1 DHCP Relay Agent Information

The switch can add information to client DHCP requests that it relays to a DHCP server. This helps provide authentication about the source of the requests. You can also specify additional information for the switch to add to the client DHCP requests that it relays to the DHCP server. Please refer to RFC 3046 for more details.

The DHCP relay agent information feature adds an Agent Information field to the option 82 field of the DHCP headers of client DHCP request frames that the switch relays to a DHCP server. The following lists the DHCP relay agent option 82 information that the switch sends to the DHCP server:

- Slot ID (1 byte)
- Port ID (1 byte)
- VLAN ID (2 bytes)
- System name (up to 32 bytes, this is optional)

24.2 Configuring DHCP Relay

Click **Routing Protocol > DHCP Relay** in the navigation panel. Use this screen to enable DHCP relay on the switch and specify the IP address(es) of the DHCP server(s).

Figure 71 DHCP Relay

The screenshot shows the DHCP Relay configuration interface. It includes a title bar, an 'Active' checkbox, three 'Remote DHCP Server' fields (all set to 0.0.0.0), a 'Relay Agent Information' section with an 'Option 82' checkbox, and an 'Information' section with a checkbox and a field showing 'VES-1616F-35'. 'Apply' and 'Cancel' buttons are at the bottom.

The following table describes the labels in this screen.

Table 57 DHCP Relay

LABEL	DESCRIPTION
Active	Select this check box to enable DHCP relay settings.
Remote DHCP Server 1.. 3	Enter the IP address(es) of the DHCP server(s).
Relay Agent Information	Select the Option 82 check box to have the switch add information (slot number, port number and VLAN ID) to client DHCP requests that it relays to a DHCP server.
Information	This read-only field displays the system name you configure in the General Setup screen. Select the check box for the switch to add the system name to client DHCP requests that it relays to a DHCP server.
Apply	Click Apply to save the changes.
Cancel	Click Cancel to reset the fields to your previous configurations.

PART V

Management

Maintenance (169)
Access Control (179)
Diagnostic (191)
Syslog (193)
Cluster Management (197)
MAC Table (203)
ARP Table (205)

Maintenance

This chapter explains how to configure the maintenance screens that let you maintain the firmware and configuration files.

25.1 The Maintenance Screen

The maintenance screens can allow you to upload new firmware (to the switch), manage configuration, reset to factory defaults and restart your switch.

Click **Management** > **Maintenance** in the navigation panel to open the screen as shown next.

Figure 72 Maintenance



The following table describes the links in this screen.

Table 58 Maintenance

LINK	DESCRIPTION
Remote Device Upgrade	Access this screen to perform remote firmware upgrade on the connected non-manageable CPE device(s).
VDSL Chip Reset	Access this screen to reset the VDSL chip(s) on this switch.
Remote Device Reset	Access this screen to reset the VDSL link(s) to the CPE device(s).
Firmware Upgrade	Access this screen to upload a new firmware to this switch.
Restore Configuration	Access this screen to upload a previously saved configuration file to the switch.
Backup Configuration	Access this screen to back up the current switch configuration.

Table 58 Maintenance (continued)

LINK	DESCRIPTION
Load Factory Default	Click this button to clear all user-entered configuration information and return the switch to its factory defaults. You may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1).
Reboot System	Click this button to restart the switch without turning the power off. This does not affect the switch's configuration.

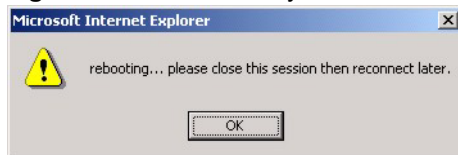
25.2 Load Factory Default

Follow the steps below to reset the switch back to the factory defaults.

- 1 In the **Maintenance** screen, click the **Click Here** button next to **Load Factory Defaults** to clear all switch configuration information you configured and return to the factory defaults. The following message appears.

Figure 73 Load Factory Default: Conformation

- 2 Click **OK** to display the screen shown next.

Figure 74 Load Factory Default: Start

- 3 Click **OK** to begin resetting all switch configurations to the factory defaults and then wait for the switch to restart. This takes up to two minutes. If you want to access the switch web configurator again, you may need to change the IP address of your computer to be in the same subnet as that of the default switch IP address (192.168.1.1).

25.3 Reboot System

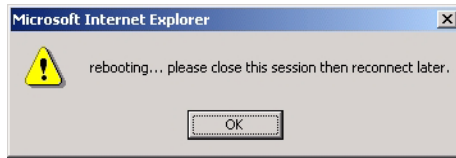
Reboot System allows you to restart the switch without physically turning the power off. Follow the steps below to reboot the switch.

- 1 In the **Maintenance** screen, click the **Click Here** button next to **Reboot System** to display the next screen.

Figure 75 Reboot System: Confirmation

- 2 Click **OK** to display the screen shown next.

Figure 76 Reboot System: Start



- 3 Click **OK** again and then wait for the switch to restart. This takes up to two minutes. This does not affect the switch's configuration.

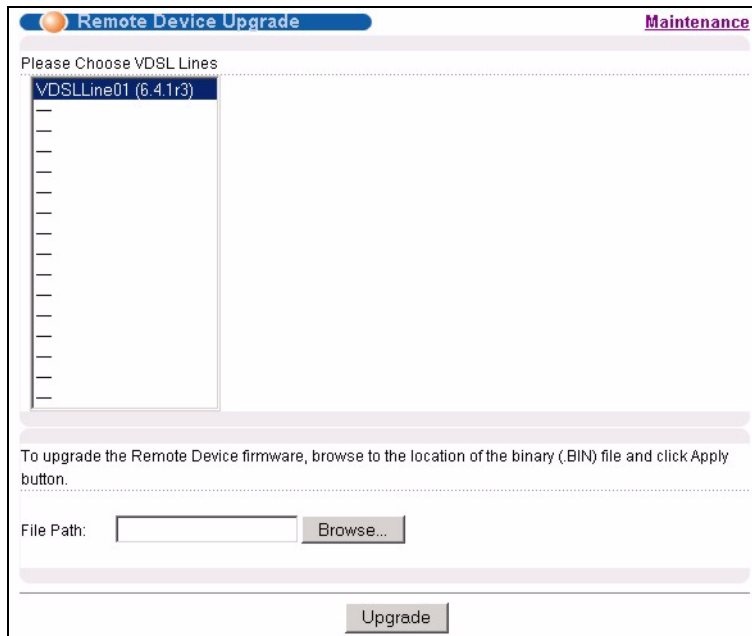
25.4 Remote Device Upgrade

The switch allows you to perform remote firmware upgrade on the connected CPE device(s). Click **Management** and **Maintenance**, then click the **Click Here** link next to **Remote Device Upgrade** to display the screen as shown next.



Be sure to upload the correct model firmware as uploading the wrong model firmware may damage the device.

Figure 77 Maintenance: Remote Device Upgrade



Follow the steps below to perform remote firmware upgrade on the CPE devices connected to the switch.

- 1 Download the latest firmware for the CPE device from www.zyxel.com and save it on a computer connected to the switch.

- 2 In the **Remote Device Upgrade** screen, select the VDSL line(s) of the CPE device(s) to which you want to upgrade the firmware. You can select multiple CPE devices by holding down the [SHIFT] or [CTRL] key and clicking the mouse at the same time.
- 3 Type the path and file name of the firmware file you wish to upload to the switch in the **File Path** text box or click **Browse** to locate it.
- 4 After you have specified the file, click **Upgrade**.

25.5 VDSL Chip Reset

There are four VDSL chips in the switch and each VDSL chip controls four VDSL ports. You can reset the VDSL chip(s) using the **VDSL Chip Reset** screen.



Resetting VDSL chip(s) disconnects the associated VDSL line(s).



Resetting the VDSL chip(s) does NOT restart the switch.

Follow the steps below to reset VDSL chips in the switch.

- 1 Access the **VDSL Chip Reset** screen from the **Maintenance** screen.

Figure 78 Maintenance: VDSL Chip Reset

- 2 Select the VDSL chips you want to reset in the list box. You can select multiple entries by holding down the [SHIFT] or [CTRL] key.
- 3 Click **Reset** to reset the selected VDSL chip(s).

25.6 Remote Device Reset

Use the **Remote Device Reset** screen to reset the VDSL line. The switch re-negotiates the VDSL link to the remote CPE device.

- 1 Access the **Remote Device Reset** screen from the **Maintenance** screen.

Figure 79 Maintenance: Remote Device Reset

- 2 Select the VDSL line(s) you want to reset in the list box. You can select multiple entries by holding down the [SHIFT] or [CTRL] key.
- 3 Click **Reset** to reset the selected VDSL line(s).



Resetting the VDSL lines does NOT restart the switch.

25.7 Firmware Upgrade



You can only upload the firmware of the same VDSL standard as your Switch. Use the `show hardware-version` command to check whether your device is a VDSL1 switch (100100, or 10050) or VDSL2 switch (5030). See [Chapter 1 on page 31](#) and [Chapter 32 on page 209](#) for more information.

Table 59 Switch Hardware Version

HARDWARE VERSION	STANDARD
100100	VDSL1
10050	VDSL1
5030	VDSL2

Make sure you have downloaded (and unzipped) the correct model firmware and version to your computer before uploading to the device.



Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

From the **Maintenance** screen, display the **Firmware Upgrade** screen as shown next.



Firmware upgrade using the web configurator saves the new firmware to ras-0.

Figure 80 Firmware Upgrade

Type the path and file name of the firmware file you wish to upload to the switch in the **File Path** text box or click **Browse** to locate it. After you have specified the file, click **Upgrade**.

After the firmware upgrade process is complete, see the **System Info** screen to verify your current firmware version number.

25.8 Restore a Configuration File

Restore a previously saved configuration from your computer to the switch using the **Restore Configuration** screen.

Figure 81 Restore Configuration

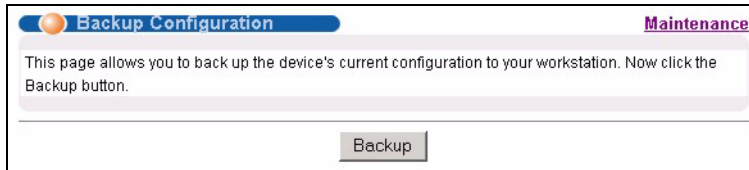
Type the path and file name of the configuration file you wish to restore in the **File Path** text box or click **Browse** to display the **Choose File** screen (below) from which you can locate it. After you have specified the file, click **Restore**. "config" is the name of the configuration file on the switch, so your backup configuration file is automatically renamed when you restore using this screen.

25.9 Backing Up a Configuration File

Backing up your switch configurations allows you to create various "snap shots" of your device from which you may restore at a later date.

Back up your current switch configuration to a computer using the **Backup Configuration** screen.

Figure 82 Backup Configuration



Follow the steps below to back up the current switch configuration to your computer in this screen.

- 1 Click **Backup**.
- 2 Click **Save** to display the **Save As** screen.
- 3 Choose a location to save the file on your computer from the **Save in** drop-down list box and type a descriptive name for it in the **File name** list box. Click **Save** to save the configuration file to your computer.

25.10 FTP Command Line

This section shows some examples of uploading to or downloading files from the switch using FTP commands. First, understand the filename conventions.

25.10.1 Filename Conventions

The configuration file (also known as the romfile or ROM) contains the factory default settings in the screens such as password, switch setup, IP Setup, etc.. Once you have customized the switch's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the “ras” file) is the system firmware and has a “bin” filename extension.

Table 60 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	config		This is the configuration filename on the switch. Uploading the config file replaces the specified configuration file system, including your switch configurations, system-related data (including the default password), the error log and the trace log.
Firmware	ras	*.bin	This is the generic name for the ZyNOS firmware on the switch.

25.10.1.1 Example FTP Commands

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file "firmware.bin" to the switch.

```
ftp> get config config.cfg
```

This is a sample FTP session saving the current configuration to a file called “config.cfg” on your computer.

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the switch only recognizes “config” and “ras”. Be sure you keep unaltered copies of both files for later use.



Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

25.10.2 FTP Command Line Procedure

- 1 Launch the FTP client on your computer.
- 2 Enter `open`, followed by a space and the IP address of your switch.
- 3 Press [ENTER] when prompted for a username.
- 4 Enter your password as requested (the default is “1234”).
- 5 Enter `bin` to set transfer mode to binary.
- 6 Use `put` to transfer files from the computer to the switch, for example, `put firmware.bin ras` transfers the firmware on your computer (firmware.bin) to the switch and renames it to “ras”. Similarly, `put config.cfg config` transfers the configuration file on your computer (config.cfg) to the switch and renames it to “config”. Likewise `get config config.cfg` transfers the configuration file on the switch to your computer and renames it “config.cfg.” See [Table 60 on page 175](#) for more information on filename conventions.
- 7 Enter `quit` to exit the ftp prompt.

25.10.3 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode. Configuration and firmware files should be transferred in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

25.10.4 FTP Restrictions

FTP will not work when:

- FTP service is disabled in the **Access Control** screen.
- The IP address(es) in the **Secured Client Set** in the **Remote Management** screen does not match the client IP address. If it does not match, the switch will disconnect the Telnet session immediately.

Access Control

This chapter describes how to control access to the switch.

26.1 Access Control Overview

The console port and FTP are allowed one session each, Telnet and SSH share four sessions, up to five web management sessions (five different usernames and passwords) and/or limitless SNMP access control sessions are allowed.

Table 61 Access Control Overview

	Console Port	SSH	Telnet	FTP	Web	SNMP
Number of concurrent sessions allowed	1	SSH and Telnet share 4 sessions.		1	5	No limit

When multiple login is disabled and there is already a console port session, you cannot telnet to the switch. The following error message displays.

```
Connection to host lost.

C:\>
```

If you disable multiple login while another administrator is accessing the switch via telnet, the switch will immediately log out the administrator and disconnect the telnet session. The following error message displays.

```
multi-login is disabled, please exit immediately!!

Connection to host lost.

C:\>
```

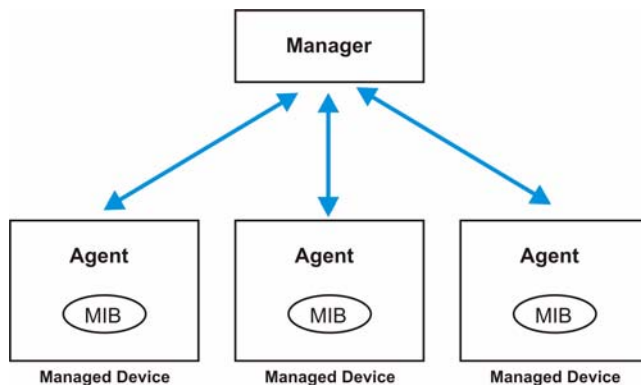
26.2 The Access Control Main Screen

Click **Management > Access Control** in the navigation panel to display the main screen as shown. Use these links to configure remote management options and create user accounts on the switch.

Figure 83 Access Control

26.3 About SNMP

Simple Network Management Protocol (SNMP) is an application layer protocol used to manage and monitor TCP/IP-based devices. SNMP is used to exchange management information between the network management system (NMS) and a network element (NE). A manager station can manage and monitor the switch through the network via SNMP version one (SNMPv1) and/or SNMP version 2c. The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

Figure 84 SNMP Management Model

An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed switch (this device). An agent translates the local management information from the managed switch into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a switch. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

Table 62 SNMP Commands

COMMAND	DESCRIPTION
Get	Allows the manager to retrieve an object variable from the agent.
GetNext	Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
Set	Allows the manager to set values for object variables within an agent.
Trap	Used by the agent to inform the manager of some events.

26.3.1 Supported MIBs

MIBs let administrators collect statistics and monitor status and performance.

The switch supports the following MIBs:

- SNMP MIB II (RFC 1213)
- RFC 1155 SMI
- RFC 1157 SNMP v1
- RFC 1493 Bridge MIBs
- RFC 1643 Ethernet MIBs
- RFC 1757 RMON
- RFC 2233 ifVHCPacketGroup
- RFC 2674 SNMPv2, SNMPv2c
- RFC 2925 PING-MIB and TRACEROUTE-MIB
- RFC 3728 VDSL line MIB
- SNMPv2, SNMPv2c or later version, compliant with RFC 2011 SNMPv2 MIB for IP, RFC 2012 SNMPv2 MIB for TCP, RFC 2013 SNMPv2 MIB for UDP

26.3.2 SNMP Traps

The switch sends traps to an SNMP manager when an event occurs. SNMP traps supported are outlined in the following table.

Table 63 SNMP Traps

OBJECT LABEL	OBJECT ID	DESCRIPTION
SNMPv2 Trap		
Cold Start	1.3.6.1.6.3.1.1.5.1	This trap is sent when the switch is turned on.
WarmStart	1.3.6.1.6.3.1.1.5.2	This trap is sent when the switch restarts.
linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
authenticationFailure	1.3.6.1.6.3.1.1.5.5	This trap is sent when an SNMP request comes from non-authenticated hosts.
RFC 1493 Traps		

Table 63 SNMP Traps (continued)

OBJECT LABEL	OBJECT ID	DESCRIPTION
newRoot	1.3.6.1.2.1.17.0.1	This trap is sent when the STP root switch changes.
topologyChange	1.3.6.1.2.1.17.0.2	This trap is sent when the STP topology changes.

26.3.3 Configuring SNMP

From the **Access Control** screen, display the **SNMP** screen. You can click **Access Control** to go back to the **Access Control** screen.

Figure 85 Access Control: SNMP

The following table describes the labels in this screen.

Table 64 Access Control: SNMP

LABEL	DESCRIPTION
Get Community	Enter the get community, which is the password for the incoming Get- and GetNext-requests from the management station.
Set Community	Enter the set community, which is the password for incoming Set- requests from the management station.
Trap Community	Enter the trap community, which is the password sent with each trap to the SNMP manager.
Trap Destination	Enter the IP addresses of up to four stations to send your SNMP traps to.
Apply	Click Apply to save your changes back to the switch.
Cancel	Click Cancel to begin configuring this screen afresh.

26.4 Setting Up Login Accounts

Up to five people (one administrator and four non-administrators) may access the switch via web configurator at any one time.

- An administrator is someone who can both view and configure switch changes. The username for the Administrator is always **admin**. The default administrator password is **1234**.



It is highly recommended that you change the default administrator password (**1234**).

- A non-administrator (username is something other than **admin**) is someone who can view but not configure switch settings.

Click **Access Control** from the navigation panel and then click **Logins** from this screen.

Figure 86 Access Control: Logins

The following table describes the labels in this screen.

Table 65 Access Control: Logins

LABEL	DESCRIPTION
Administrator	This is the default administrator account with the “admin” user name. You cannot change the default administrator user name. Only the administrator has read/write access.
Old Password	Type the existing system password (1234 is the default password when shipped).
New Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation
Edit Logins	You may configure passwords for up to four users. These people have read-only access.
User Name	Set a user name (up to 30 characters long).
Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation
Apply	Click Apply to save your changes back to the switch.
Cancel	Click Cancel to begin configuring this screen afresh.

26.5 SSH Overview

Unlike Telnet or FTP, which transmit data in clear text, SSH (Secure Shell) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

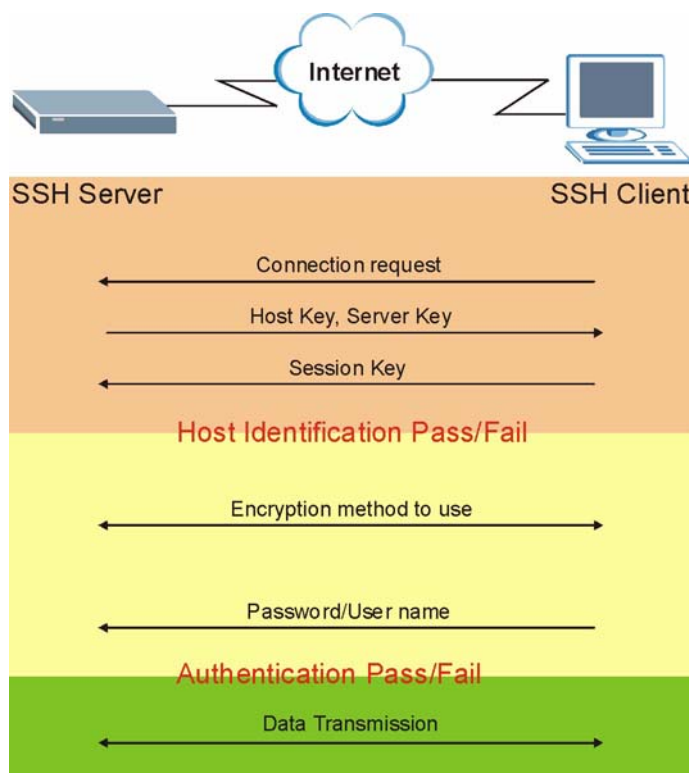
Figure 87 SSH Communication Example



26.6 How SSH works

The following table summarizes how a secure connection is established between two remote hosts.

Figure 88 How SSH Works



1 Host Identification

The SSH client sends a connection request to the SSH server. The server identifies itself with a host key. The client encrypts a randomly generated session key with the host key and server key and sends the result back to the server.

The client automatically saves any new server public keys. In subsequent connections, the server public key is checked against the saved version on the client computer.

2 Encryption Method

Once the identification is verified, both the client and server must agree on the type of encryption method to use.

3 Authentication and Data Transmission

After the identification is verified and data encryption activated, a secure tunnel is established between the client and the server. The client then sends its authentication information (user name and password) to the server to log in to the server.

26.7 SSH Implementation on the Switch

Your switch supports SSH version 2 using RSA authentication and three encryption methods (DES, 3DES and Blowfish). The SSH server is implemented on the switch for remote management and file transfer on port 22.

26.7.1 Requirements for Using SSH

You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the switch over SSH.

26.7.2 SSH Login Example

You can use an SSH client program to access the switch. The following figure shows an example using a text-based SSH client program. Refer to the documentation that comes with your SSH program for information on using it.

Figure 89 SSH Login Example

```

C:\>ssh2 admin@192.168.1.1
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@          WARNING: HOST IDENTIFICATION HAS CHANGED!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the host key has just been changed.
Please contact your system administrator.
Add correct host key to "C:/Documents and Settings/Administrator/Application
Data/SSH/hostkeys/key_22_192.168.1.1.pub" to get rid of this message.
Received server key's fingerprint: xigil-gidot-homug-duzab-tocyh-pamyb-
ronep-tisaf-hebip-gokeb-goxix You can get a public key's fingerprint by
running % ssh-keygen -F publickey.pub
on the keyfile. Agent forwarding is disabled to avoid attacks by corrupted
servers. X11 forwarding is disabled to avoid attacks by corrupted servers.
Are you sure you want to continue connecting (yes/no)? yes

Do you want to change the host key on disk (yes/no)? yes

Agent forwarding re-enabled.
X11 forwarding re-enabled.
Host key saved to C:/Documents and Settings/Administrator/Application Data/
SSH/hostkeys/key_22_192.168.1.1.pub host key for 192.168.1.1, accepted by
Administrator Thu May 12 2005 09:52:21
admin's password:
Authentication successful.
Copyright (c) 1994 - 2005 ZyXEL Communications Corp.
sysname>

```

26.8 Introduction to HTTPS

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

It relies upon certificates, public keys, and private keys.

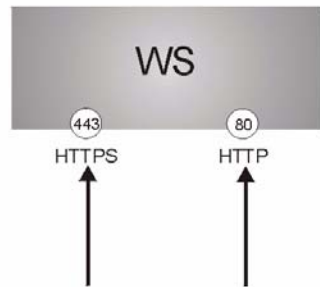
HTTPS on the switch is used so that you may securely access the switch using the web configurator. The SSL protocol specifies that the SSL server (the switch) must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the switch), whereas the SSL client only should authenticate itself when the SSL server requires it to do so. Authenticating client certificates is optional and if selected means the SSL-client must send the switch a certificate. You must apply for a certificate for the browser from a CA that is a trusted CA on the switch.

Please refer to the following figure.

- 1 HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the switch's WS (web server).

- 2 HTTP connection requests from a web browser go to port 80 (by default) on the switch's WS (web server).

Figure 90 HTTPS Implementation



If you disable **HTTP** in the **Service Access Control** screen, then the switch blocks all HTTP connection attempts.

26.9 HTTPS Example

If you haven't changed the default HTTPS port on the switch, then in your browser enter "https://switch IP Address/" as the web site address where "switch IP Address" is the IP address or domain name of the switch you wish to access.

26.9.1 Internet Explorer Warning Messages

When you attempt to access the switch HTTPS server, a Windows dialog box pops up asking if you trust the server certificate. Click **View Certificate** if you want to verify that the certificate is from the switch.

You see the following **Security Alert** screen in Internet Explorer. Select **Yes** to proceed to the web configurator login screen; if you select **No**, then web configurator access is blocked.

Figure 91 Security Alert Dialog Box (Internet Explorer)



26.9.2 Netscape Navigator Warning Messages

When you attempt to access the switch HTTPS server, a **Website Certified by an Unknown Authority** screen pops up asking if you trust the server certificate. Click **Examine Certificate** if you want to verify that the certificate is from the switch.

If **Accept this certificate temporarily for this session** is selected, then click **OK** to continue in Netscape.

Select **Accept this certificate permanently** to import the switch's certificate into the SSL client.

Figure 92 Security Certificate 1 (Netscape)

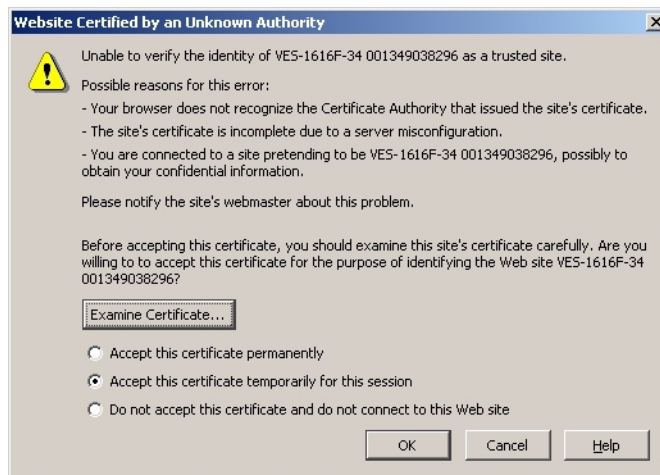
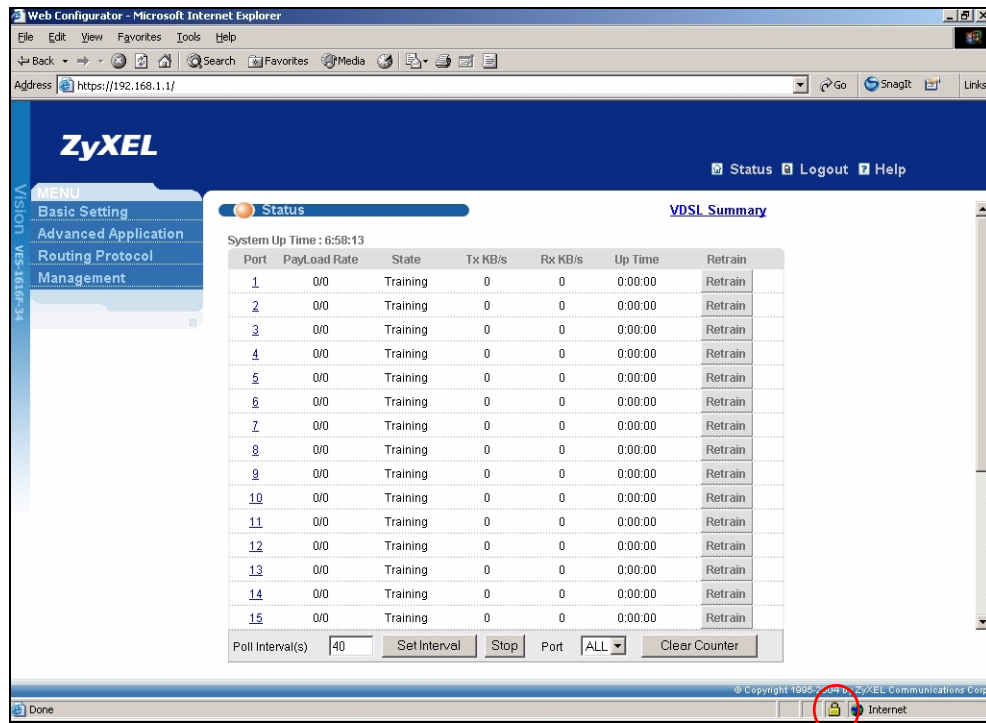


Figure 93 Security Certificate 2 (Netscape)



26.9.3 The Main Screen

After you accept the certificate and enter the login username and password, the switch main screen appears. The lock displayed in the bottom right of the browser status bar denotes a secure connection.

Figure 94 Example: Lock Denoting a Secure Connection

26.10 Service Access Control

Service Access Control allows you to decide what services you may use to access the switch. You may also change the default service port and configure “trusted computer(s)” for each service in the **Remote Management** screen (discussed later). Click **Access Control** to go back to the main **Access Control** screen.

Figure 95 Access Control: Service Access Control

The screenshot shows the 'Service Access Control' screen. It has a table with the following data:

Services	Active	Service Port	Timeout
Telnet	<input checked="" type="checkbox"/>	23	
SSH	<input checked="" type="checkbox"/>	22	
FTP	<input checked="" type="checkbox"/>	21	
HTTP	<input checked="" type="checkbox"/>	80	3 Minutes
HTTPS	<input checked="" type="checkbox"/>	443	
ICMP	<input checked="" type="checkbox"/>		
SNMP	<input checked="" type="checkbox"/>		

At the bottom are 'Apply' and 'Cancel' buttons.

The following table describes the fields in this screen.

Table 66 Access Control: Service Access Control

LABEL	DESCRIPTION
Services	Services you may use to access the switch are listed here.
Active	Select this option for the corresponding services that you want to allow to access the switch.

Table 66 Access Control: Service Access Control (continued)

LABEL	DESCRIPTION
Service Port	For Telnet, SSH, FTP, HTTP or HTTPS services, you may change the default service port by typing the new port number in the Server Port field. If you change the default port number then you will have to let people (who wish to use the service) know the new port number for that service.
Timeout	Type how many minutes a management session (via the web configurator) can be left idle before the session times out. After it times out you have to log in with your password again. Very long idle timeouts may have security risks.
Apply	Click Apply to save your changes back to the switch.
Cancel	Click Cancel to begin configuring this screen afresh.

26.11 Remote Management

From the **Access Control** screen, display the **Remote Management** screen as shown next.

You can specify a group of one or more “trusted computers” from which an administrator may use a service to manage the switch. Click **Access Control** to return to the **Access Control** screen.

Figure 96 Access Control: Remote Management

Entry	Active	Start Address	End Address	Telnet	FTP	Web	ICMP	SNMP	SSH	HTTPS
1	<input checked="" type="checkbox"/>	0.0.0.0	0.0.0.0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Apply Cancel

The following table describes the labels in this screen.

Table 67 Access Control: Remote Management

LABEL	DESCRIPTION
Entry	This is the client set index number. A “client set” is a group of one or more “trusted computers” from which an administrator may use a service to manage the switch.
Active	Select this check box to activate this secured client set. Clear the check box if you wish to temporarily disable the set without deleting it.
Start Address End Address	Configure the IP address range of trusted computers from which you can manage this switch. The switch checks if the client IP address of a computer requesting a service or protocol matches the range set here. The switch immediately disconnects the session if it does not match.
Telnet/FTP/ Web/ICMP/ SNMP/SSH/ HTTPS	Select services that may be used for managing the switch from the specified trusted computers.
Apply	Click Apply to save your changes back to the switch.
Cancel	Click Cancel to begin configuring this screen afresh.

Diagnostic

This chapter explains the **Diagnostic** screen.

27.1 Diagnostic

Click **Management** > **Diagnostic** in the navigation panel to open this screen. Use this screen to check system logs, reset the system or ping IP addresses.

Figure 97 Diagnostic

The screenshot shows the 'Diagnostic' screen with a title bar containing an orange circle icon and the word 'Diagnostic'. Below the title bar is a large multi-line text box labeled '- Info -'. At the bottom of the screen, there are three sections: 'System Log' with 'Display' and 'Clear' buttons; 'IP Ping' with an 'IP Address' input field and a 'Ping' button; and 'Port Test' with a 'Port' dropdown menu (showing '1'), 'Internal Test' and 'External Test' buttons.

The following table describes the labels in this screen.

Table 68 Diagnostic

LABEL	DESCRIPTION
System Log	Click Display to display a log of events in the multi-line text box. Click Clear to empty the text box and reset the syslog entry.
IP Ping	Type the IP address of a device that you want to ping in order to test a connection. Click Ping to have the switch ping the IP address (in the field to the left).
Port Test	From the Port drop-down list box, select a port number and click Internal Test to perform internal loopback test or click External Test (on VDSL ports) to perform loopback test to the remote devices.

Syslog

This chapter explains the syslog screens.

28.1 Syslog Overview

The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event messages. A syslog-enabled device can generate a syslog message and send it to a syslog server.

Syslog is defined in RFC 3164. The RFC defines the packet format, content and system log related information of syslog messages. Each syslog message has a facility and severity level. The syslog facility identifies a file in the syslog server. Refer to the documentation of your syslog program for details. The following table describes the syslog severity levels.

Table 69 Syslog Severity Levels

CODE	SEVERITY
0	Emergency: The system is unusable.
1	Alert: Action must be taken immediately.
2	Critical: The system condition is critical.
3	Error: There is an error condition on the system.
4	Warning: There is a warning condition on the system.
5	Notice: There is a normal but significant condition on the system.
6	Informational: The syslog contains an informational message.
7	Debug: The message is intended for debug-level purposes.

28.2 Syslog Setup

Click **Management** and then **Syslog** in the navigation panel to display this screen. The syslog feature sends logs to an external syslog server. Use this screen to configure the device's system logging settings.

Figure 98 Syslog Setup

Logging type	Active	Facility
System	<input type="checkbox"/>	local use 0
Interface	<input type="checkbox"/>	local use 0
Switch	<input type="checkbox"/>	local use 0
Authentication	<input type="checkbox"/>	local use 0
IP	<input type="checkbox"/>	local use 0

The following table describes the labels in this screen.

Table 70 Syslog

LABEL	DESCRIPTION
Syslog	Select Active to turn on syslog (system logging) and then configure the syslog setting
Logging Type	This column displays the names of the categories of logs that the device can generate.
Active	Select this option to set the device to generate logs for the corresponding category.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Apply	Click Apply to save your changes back to the device.
Cancel	Click Cancel to begin configuring this screen afresh.

28.3 Syslog Server Setup

Click **Management** and then **Syslog** in the navigation panel to display the **Syslog Setup** screen. Click the **Syslog Server Setup** link to open the following screen. Use this screen to configure a list of external syslog servers.

Figure 99 Syslog Server Setup

The screenshot shows the 'Syslog Server Setup' configuration interface. It includes a title bar with the text 'Syslog Server Setup' and a link 'Syslog Setup'. The main configuration area contains three fields: 'Active' (a checkbox that is currently unchecked), 'Server Address' (a text box containing '0.0.0.0'), and 'Log Level' (a dropdown menu currently set to 'Level 0'). Below these fields are three buttons: 'Add', 'Cancel', and 'Clear'. At the bottom of the screen, there is a table with the following columns: 'Index', 'Active', 'IP Address', 'Log Level', and 'Delete'. Below the table are two buttons: 'Delete' and 'Cancel'.

The following table describes the labels in this screen.

Table 71 Syslog Server Setup

LABEL	DESCRIPTION
Active	Select this check box to have the device send logs to this syslog server. Clear the check box if you want to create a syslog server entry but not have the device send logs to it (you can edit the entry later).
Server Address	Enter the IP address of the syslog server.
Log Level	Select the severity level(s) of the logs that you want the device to send to this syslog server. The lower the number, the more critical the logs are.
Add	Click Add to save your changes back to the device. The entry displays in the table below.
Cancel	Click Cancel to begin configuring this screen afresh.
Clear	Click Clear to return the fields to the factory defaults.
Index	This is the index number of a syslog server entry. Click this number to edit the entry.
Active	This field displays Yes if the device is to send logs to the syslog server. No displays if the device is not to send logs to the syslog server.
IP Address	This field displays the IP address of the syslog server.
Log Level	This field displays the severity level of the logs that the device is to send to this syslog server.
Delete	Select an entry's Delete check box and click Delete to remove the entry.
Cancel	Click Cancel to begin configuring this screen afresh.

Cluster Management

This chapter introduces cluster management.

29.1 Cluster Management Overview

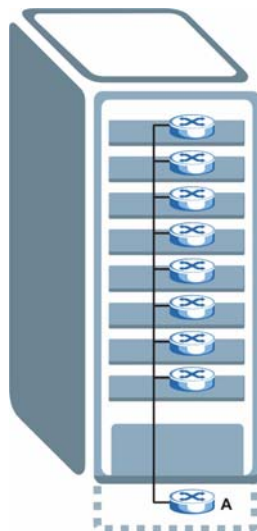
Cluster Management allows you to manage switches through one switch, called the cluster manager. The switches must be directly connected and be in the same VLAN group so as to be able to communicate with one another.

Table 72 ZyXEL Clustering Management Specifications

Maximum number of cluster members	24
Cluster Member Models	Must be compatible with ZyXEL cluster management implementation.
Cluster Manager	The switch through which you manage the cluster member switches.
Cluster Members	The switches being managed by the cluster manager switch.

In the following example, switch **A** in the basement is the cluster manager and the other switches on the upper floors of the building are cluster members.

Figure 100 Clustering Application Example



29.2 Cluster Management Status

Click **Management > Cluster Management** in the navigation panel to display the following screen.



A cluster can only have one manager.

Figure 101 Cluster Management Status

Clustering Management Status

Configuration

Status	Manager
Manager	00:19:cb:00:00:02

The Number Of Member = 1

Index	MacAddr	Name	Model	Status
1	00:13:49:00:00:02	VES-1608FA-35	VES-1608FA-35	Online

The following table describes the labels in this screen.

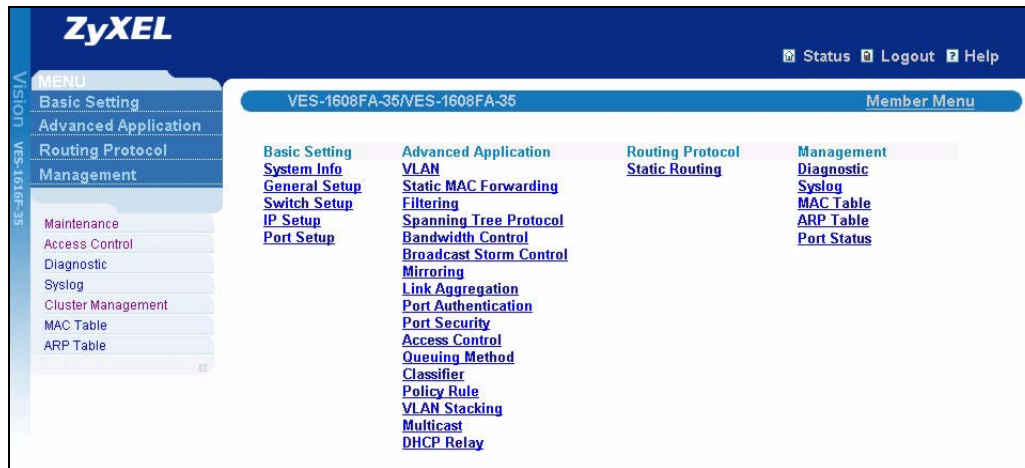
Table 73 Cluster Management Status

LABEL	DESCRIPTION
Status	This field displays the role of this switch within the cluster. Manager Member (you see this if you access this screen in the cluster member switch directly and not via the cluster manager) None (neither a manager nor a member of a cluster)
Manager	This field displays the cluster manager switch's hardware MAC address.
The Number of Member	This field displays the number of switches that make up this cluster. The following fields describe the cluster member switches.
Index	You can manage cluster member switches via the cluster manager switch. Each number in the Index column is a hyperlink leading to the cluster member switch's web configurator (see Figure 102 on page 199).
MacAddr	This is the cluster member switch's hardware MAC address.
Name	This is the cluster member switch's System Name .
Model	This field displays the model name.
Status	This field displays: Online (the cluster member switch is accessible) Error (for example the cluster member switch password was changed or the switch was set as the manager and so left the member list, etc.) Offline (the switch is disconnected - Offline shows approximately 1.5 minutes after the link between cluster member and manager goes down)

29.2.1 Cluster Member Switch Management

Go to the **Clustering Management Status** screen of the cluster manager switch and then click on an **Index** hyperlink from the list of members to go to that cluster member switch's web configurator home page. This cluster member web configurator home page and the home page that you'd see if you accessed it directly are different.

Figure 102 Cluster Management: Cluster Member Web Configurator Screen



29.2.1.1 Uploading Firmware to a Cluster Member Switch

You can use FTP to upload firmware to a cluster member switch through the cluster manager switch as shown in the following example.

Figure 103 Example: Uploading Firmware to a Cluster Member Switch

```
C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220  FTP version 1.0 ready at Thu Jan  1 00:47:52 1970
User (192.168.1.1:(none)): admin
331 Enter PASS command
Password:
230 Logged in
ftp> ls
200 Port command okay
150 Opening data connection for LIST
--w--w--w-  1 owner   group      1459070 Jul  01 12:00 ras
-rw-rw-rw-   1 owner   group        49152 Jul  01 12:00 config
--w--w--w-  1 owner   group           0 Jul  01 12:00 fw-00-13-49-00-00-01
-rw-rw-rw-   1 owner   group           0 Jul  01 12:00 config-00-13-49-00-00-01
226 File sent OK
ftp: 297 bytes received in 0.01Seconds 19.80Kbytes/sec.
ftp> bin
200 Type I OK
ftp> put 360AIH0.bin fw-00-13-49-00-00-01
200 Port command okay
150 Opening data connection for STOR fw-00-13-49-00-00-01
226 File received OK
ftp: 262144 bytes sent in 0.63Seconds 415.44Kbytes/sec.
ftp>
```

The following table explains some of the FTP parameters.

Table 74 FTP Upload to Cluster Member Example

FTP PARAMETER	DESCRIPTION
User	Enter "admin".
Password	The web configurator password default is 1234.
ls	Enter this command to list the name of cluster member switch's firmware and configuration file.
360AIH0.bin	This is the name of the firmware file you want to upload to the cluster member switch.
fw-00-13-49-00-00-01	This is the cluster member switch's firmware name as seen in the cluster manager switch.
config-00-13-49-00-00-01	This is the cluster member switch's configuration file name as seen in the cluster manager switch.

29.3 Configuring Cluster Management

Click **Configuration** from the **Cluster Management** screen to display the next screen.

Refer to [Section 29.1 on page 197](#) for more information.

Figure 104 Clustering Management Configuration

Clustering Management Configuration Status

Clustering Manager:

Active ☒

Name

VID

Apply Cancel

Clustering Candidate:

List

Password

Add Cancel Refresh

Index	MacAddr	Name	Model	Remove

Remove Cancel

The following table describes the labels in this screen.

Table 75 Clustering Management Configuration

LABEL	DESCRIPTION
Clustering Manager	
Active	Select Active to have this switch become the cluster manager switch. A cluster can only have one manager. Other (directly connected) switches that are set to be cluster managers will not be visible in the Clustering Candidates list. If a switch that was previously a cluster member is later set to become a cluster manager, then its Status is displayed as Error in the Cluster Management Status screen and a warning icon (⚠) appears in the member summary list below.
Name	Type a name to identify the Clustering Manager . You may use up to 32 printable characters (spaces are allowed).
VID	This is the VLAN ID and is only applicable if the switch is set to 802.1Q VLAN. All switches must be directly connected and in the same VLAN group to belong to the same cluster. Switches that are not in the same VLAN group are not visible in the Clustering Candidates list. This field is ignored if the Clustering Manager is using Port-based VLAN.
Apply	Click Apply to save your changes to the switch.
Cancel	Click Cancel to begin configuring this part of the screen afresh.
Clustering Candidate	The following fields relate to the switches that are potential cluster members.
List	A list of suitable candidates found by auto-discovery is shown here. The switches must be directly connected. Directly connected switches that are set to be cluster managers will not be visible in the Clustering Candidate list. Switches that are not in the same management VLAN group will not be visible in the Clustering Candidate list.
Password	Each cluster member's password is its web configurator password. Select a member in the Clustering Candidate list and then enter its web configurator password. If that switch administrator changes the web configurator password afterwards, then it cannot be managed from the Cluster Manager . Its Status is displayed as Error in the Cluster Management Status screen and a warning icon (⚠) appears in the member summary list below. If multiple devices have the same password then hold [SHIFT] and click those switches to select them. Then enter their common web configurator password.
Add	Click Add to save this part of the screen to the switch.
Cancel	Click Cancel to begin configuring this part of the screen afresh.
Refresh	Click Refresh to perform auto-discovery again to list potential cluster members.
The next summary table shows the information for the clustering members configured.	
Index	This is the index number of a cluster member switch.
MacAddr	This is the cluster member switch's hardware MAC address.
Name	This is the cluster member switch's System Name .
Model	This is the cluster member switch's model name.
Remove	Select this checkbox and then click the Remove button to remove a cluster member switch from the cluster.
Cancel	Click Cancel to begin configuring this part of the screen afresh.

MAC Table

This chapter introduces the **MAC Table** screen.

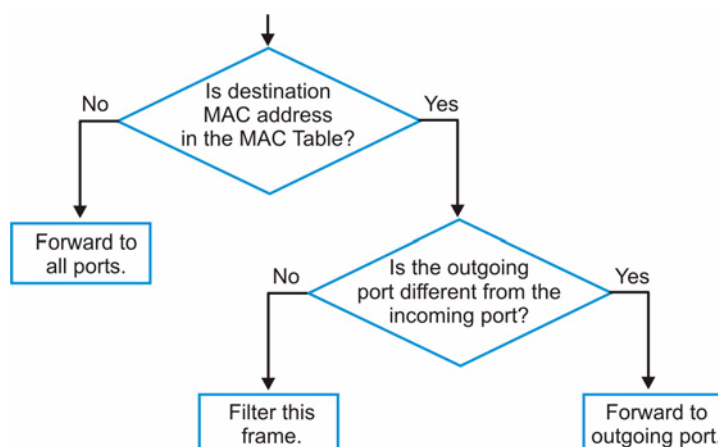
30.1 MAC Table Overview

The **MAC Table** screen (a MAC table is also known as a filtering database) shows how frames are forwarded or filtered across the switch's ports. It shows what device MAC address, belonging to what VLAN group (if any) is forwarded to which port(s) and whether the MAC address is dynamic (learned by the switch) or static (manually entered in the **Static MAC Forwarding** screen).

The switch uses the MAC table to determine how to forward frames. See the following figure.

- 1 The switch examines a received frame and learns the port on which this source MAC address came.
- 2 The switch checks to see if the frame's destination MAC address matches a source MAC address already learned in the MAC table.
 - If the switch has already learned the port for this MAC address, then it forwards the frame to that port.
 - If the switch has not already learned the port for this MAC address, then the frame is flooded to all ports. Too much port flooding leads to network congestion.
 - If the switch has already learned the port for this MAC address, but the destination port is the same as the port it came in on, then it filters the frame.

Figure 105 MAC Table Flowchart



30.2 Viewing the MAC Table

Click **Management** > **MAC Table** in the navigation panel.



Click a button in the **Sort by** field to display the MAC address table entries.

Figure 106 MAC Table

MAC Table				
Sort by	MAC	VID	Port	
Index	MAC Address	VID	Port	Type
1	00:02:e3:57:ea:4f	1	17	dynamic
2	00:04:80:9b:78:00	1	17	dynamic
3	00:0a:e4:13:7f:67	1	17	dynamic
4	00:0d:60:8f:09:a1	1	17	dynamic
5	00:0d:60:cb:3b:c9	1	17	dynamic
6	00:0ffe:32:b4:12	1	17	dynamic
7	00:10:b5:ae:56:9b	1	17	dynamic
8	00:11:85:89:7a:d9	1	17	dynamic
9	00:13:49:22:a3:3b	1	17	dynamic
10	00:16:36:10:26:c3	1	17	dynamic
11	00:16:36:16:f2:73	1	17	dynamic
12	00:50:70:12:04:39	1	17	dynamic
13	00:50:ba:ad:4f:81	1	17	dynamic
14	00:c0:9f:cd:cc:5f	1	17	dynamic
15	00:c0:a8:fa:e9:27	1	17	dynamic
16	00:d0:59:b8:10:3c	1	17	dynamic

The following table describes the labels in this screen.

Table 76 MAC Table

LABEL	DESCRIPTION
Sort by	Click one of the following buttons to display and arrange the data according to that button type. The information is then displayed in the summary table below.
MAC	Click this button to display and arrange the data according to MAC address.
VID	Click this button to display and arrange the data according to VLAN group.
Port	Click this button to display and arrange the data according to port number.
Index	This is the incoming frame index number.
MAC Address	This is the MAC address of the device from which this incoming frame came.
VID	This is the VLAN group to which this frame belongs.
Port	This is the port from which the above MAC address was learned.
Type	This shows whether the MAC address is dynamic (learned by the switch) or static (manually entered in the Static MAC Forwarding screen).

ARP Table

This chapter introduces ARP table.

31.1 ARP Table Overview

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network.

An IP (version 4) address is 32 bits long. In an Ethernet LAN, MAC addresses are 48 bits long. The ARP Table maintains an association between each MAC address and its corresponding IP address.

31.1.1 How ARP Works

When an incoming packet destined for a host device on a local area network arrives at the switch, the switch's ARP program looks in the ARP Table and, if it finds the address, sends it to the device.

If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The switch fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the switch puts all ones in the target MAC field (FF.FF.FF.FF.FF.FF is the Ethernet broadcast address). The replying device (which is either the IP address of the device being sought or the router that knows the way) replaces the broadcast address with the target's MAC address, swaps the sender and target pairs, and unicasts the answer directly back to the requesting machine. ARP updates the ARP Table for future reference and then sends the packet to the MAC address that replied.

31.2 Viewing the ARP Table

Click **Management > ARP Table** in the navigation panel to open the following screen. Use the ARP table to view IP-to-MAC address mapping(s).

Figure 107 ARP TableThe screenshot shows a web interface titled "ARP Table" with a blue header bar. Below the header is a table with four columns: Index, IP Address, MAC Address, and Type. A single row is visible with the following values: Index 1, IP Address 172.23.37.116, MAC Address 00:0f:fe:32:b4:12, and Type dynamic.

Index	IP Address	MAC Address	Type
1	172.23.37.116	00:0f:fe:32:b4:12	dynamic

The following table describes the labels in this screen.

Table 77 ARP Table

LABEL	DESCRIPTION
Index	This is the ARP Table entry number.
IP Address	This is the learned IP address of a device connected to a switch port with corresponding MAC address below.
MAC Address	This is the MAC address of the device with corresponding IP address above.
Type	This shows whether the MAC address is dynamic (learned by the switch) or static (manually entered in the Static MAC Forwarding screen).

PART VII

Commands, Troubleshooting and Specifications

Introducing the Commands (209)
Command Examples (243)
IEEE 802.1Q Tagged VLAN Commands (259)
Troubleshooting (267)
Product Specifications (275)

Introducing the Commands

This chapter introduces the commands and gives a summary of commands available.

32.1 Overview

In addition to the web configurator, you can use line commands to configure the switch. Use line commands for advanced switch diagnosis and troubleshooting. If you have problems with your switch, customer support may request that you issue some of these commands to assist them in troubleshooting.



See the web configurator parts of this User's Guide for background information on features configurable by the web configurator.

32.1.1 Switch Configuration File

When you configure the switch using either the CLI or web configurator, the settings are saved as a series of commands in a configuration file on the switch. You can perform the following with a configuration file:

- Back up switch configuration once the switch is set up to work in your network.
- Restore switch configuration.
- Use the same configuration file to set all switches (of the same model) in your network to the same settings.



You may also edit a configuration file using a text editor.



Make sure you use valid commands. The switch rejects configuration files with invalid or incomplete commands.

32.2 Accessing the CLI

You can use a direct console connection or Telnet to access the CLI on the switch.



The switch automatically logs you out of the management interface after five minutes of inactivity. If this happens to you, simply log back in again.

32.2.1 Multiple Login

You can use a direct console connection or Telnet to access the command interpreter on the switch.



The switch automatically logs you out of the management interface after five minutes of inactivity. If this happens to you, simply log back in again.

- By default, the multi-login feature is enabled to allow multiple CLI management sessions.
- Use the `configure multi-login` command in the configuration mode to allow multiple concurrent logins. However, no more than five concurrent login sessions are allowed. To disable this feature, use the `configure no multi-login` command.

32.2.2 The Console Port

Connect to the switch's console port using a terminal emulation software configured to the following settings:

- VT100 terminal emulation
- 9600 bps
- No parity
- 8 data bits
- 1 stop bit
- No flow control

32.2.2.1 Initial Screen

When you turn on your switch, it performs several internal tests as well as line initialization. You can view the initialization information using the console port. After the initialization, the login screen displays (refer to [Section 32.3 on page 212](#)).

```
Copyright (c) 1994 - 2006 ZyXEL Communications Corp.  
initialize mgmt, ethernet address: 00:13:49:01:23:45  
initialize switch, ethernet address: 00:13:49:01:23:46  
Initializing switch unit 0...  
  
Press ENTER to continue...
```

32.2.3 Telnet

Use the following steps to telnet into your switch.

- 1** For local management, connect your computer to the RJ-45 management port (labeled **MGMT**) on the switch.
- 2** Make sure your computer IP address and the switch IP address are on the same subnet. In Windows, click **Start** (usually in the bottom left corner), **Run** and then type `telnet 192.168.0.1` (the default management IP address) and click **OK**.
- 3** A login screen displays.

32.2.4 SSH

You can use an SSH client program to access the switch. The following figure shows an example using a text-based SSH client program. Refer to the documentation that comes with your SSH program for information on using it.

```
C:\>ssh2 admin@192.168.0.1
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@           WARNING: HOST IDENTIFICATION HAS CHANGED!           @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the host key has just been changed.
Please contact your system administrator.
Add correct host key to "C:/Documents and Settings/Administrator/Application
Data/SSH/hostkeys/key_22_192.168.0.1.pub" to get rid of this message.
Received server key's fingerprint: xigil-gidot-homug-duzab-tocyh-pamyb-
ronep-tisaf-hebip-gokeb-goxix You can get a public key's fingerprint by
running % ssh-keygen -F publickey.pub
on the keyfile. Agent forwarding is disabled to avoid attacks by corrupted
servers. X11 forwarding is disabled to avoid attacks by corrupted servers.
Are you sure you want to continue connecting (yes/no)? yes

Do you want to change the host key on disk (yes/no)? yes

Agent forwarding re-enabled.
X11 forwarding re-enabled.
Host key saved to C:/Documents and Settings/Administrator/Application Data/
SSH/hostkeys/key_22_192.168.0.1.pub host key for 192.168.0.1, accepted by
Administrator Thu May 12 2005 09:52:21
admin's password:
Authentication successful.
Copyright (c) 1994 - 2005 ZyXEL Communications Corp.
sysname>
```

32.3 The Login Screen

After you have successfully established a connection to the switch using a direct console connection or Telnet, a login screen displays. The following figure shows an example. For your first login, enter the default administrator login username “admin” and password “1234”.

```
Enter User Name : admin
Enter Password : XXXX
```

32.4 Command Syntax Conventions

The rules of the commands are listed next.

- The command keywords are in *courier new* font.
- The required fields in a command are enclosed in angle brackets <>, for instance, ping <ip> means that you must specify an IP number for this command.

- The optional fields in a command are enclosed in square brackets [], for instance,

```
configure snmp-server [contact <system contact>] [location
<system location>]
```

means that the `contact` and `location` fields are optional.

- “Command” refers to a command used in the command line interface (CLI command).
- The | symbol means “or”.
- The entry `<cr>` in the command lines refers to carriage return. Press [ENTER] or carriage return after a command to execute the command.
- Use the up (↑) or down (↓) arrow key to scroll through the command history list.
- The CLI does not accept partial or incomplete commands. You may enter a unique part of a command and press [TAB] to have the switch automatically display the full command. For example, if you enter “`config`” and press [TAB], the full command of “`configure`” automatically displays.
- Each interface refers to a port on the switch. Commands configured after the interface command correspond to the port.
- Type multiple ports or port ranges separated by a comma. Ranges of port numbers are typed separated by a dash.

32.5 Getting Help

The system includes a help facility to provide you with the following information about the commands:

- List of available commands under a command group.
- Detailed descriptions of the commands.

32.5.1 List of Available Commands

Enter “`help`” to display a list of available commands and the corresponding sub commands.

Enter “`?`” to display a list of commands you can use.

```
sysname> help
  Commands available:

  help
  logout
  exit
  history
  enable
  show ip <cr>
  ping <ip|host-name> <cr>
  traceroute <ip|host-name> <cr>
  ssh <1|2> <[user@]dest-ip> <cr>
  ssh <1|2> <[user@]dest-ip> [command </>]
sysname>
```

```
sysname> ?
  enable          Turn on privileged commands
  exit            Exit from the EXEC
  help            Description of the interactive help system
  history          Show a list of previously run commands
  logout          Exit from the EXEC
  ping            Exec ping
  show            Show system information
  ssh             SSH client
  traceroute      Exec traceroute
sysname>
```

32.5.2 Detailed Command Information

Enter `<command> help` to display detailed sub command and parameters.

Enter `<command> ?` to display detailed help information about the sub commands and parameters.

```
sysname> ping help
Commands available:
ping <ip>
  <
    [ in-band|out-of-band|vlan <vlan-id> ]
    [ size <0-1472> ]
    [ -t ]
  >
sysname>
```

```
sysname> ping ?
  <ip|host-name>    destination ip address
  help              Description of ping help
sysname>
```

32.6 Changing the Password

This command is used to change the password for Enable mode. By default the same password is used to enter the command line interface (CLI) and Enable and Config modes of the CLI.

The password you change with this command is required to enter Enable and Config modes of the CLI.

Syntax:

```
password <password>
```

where

<code><password></code>	= Specifies the new password (up to 32 alphanumeric characters) users have to type in to enter Enable and Config modes.
-------------------------------	---

32.7 Account Privilege Levels

You can use a command whose privilege level is equal to or less than that of your login account. For example, if your login account has a privilege level of 12, you can use all commands with privilege levels from 0 to 12. 0-privileged commands are available to all login accounts.

32.8 Command Modes

There are three command modes: User, Enable and Configure. The modes (and commands) available to you depend on what level of privilege your account has. Use the `logins username` command in Configure mode to set up accounts and privilege levels.

When you first log into the command interpreter with a read-only account (having a privilege of 0 to 12), the initial mode is User mode. The User mode commands are a subset of the Enable mode commands. The User mode command prompt ends with an angle bracket (>).

To enter Enable (or privileged) mode using a read-only account, type `enable` and enter the administrator password when prompted (the default is 1234). When you enter Enable mode, the command prompt changes to the pound sign (#). If you log into the command interpreter as an administrator you automatically enter Enable mode.

The following table describes command interpreter modes and how to access them..

Table 78 Command Interpreter Mode Summary

MODE	DESCRIPTION	HOW TO LOGIN/ACCESS	PROMPT
User	Commands available in this mode are a subset of enable mode. You can perform basic tests and display general system information.	Default login level for a read-only account.	<code>sysname></code> The first part of the prompt is the system name. In the CLI examples in this User's Guide, the system name is always "sysname".
Enable	Commands available in this mode allow you to save configuration settings, reset configuration settings as well as display further system information. This mode also contains the <code>configure</code> command which takes you to config mode.	Default login level for the administrator or accounts with a privilege of 13 or 14. Read-only accounts (with a privilege of 0 - 12) need to type the <code>enable</code> command and enter the Enable mode password.	<code>sysname#</code>
Config	Commands available in this mode allow you to configure settings that affect the switch globally.	Type <code>config</code> or <code>configure</code> in Enable mode.	<code>sysname(config)#</code>
Command modes that follow are sub-modes of the config mode and can only be accessed from within the config mode.			

Table 78 Command Interpreter Mode Summary (continued)

MODE	DESCRIPTION	HOW TO LOGIN/ ACCESS	PROMPT
Config-interface	This is a sub-mode of the config mode and allows you to configure port related settings.	Type <code>interface port-channel</code> followed by a port number. For example, <code>interface port-channel 10</code> to configure port 10 on the switch.	<code>sysname(config-interface) #</code>
Config-mvr	This is a sub-mode of the config mode and allows you to configure multicast VLAN settings.	To enter MVR mode, enter <code>mvr</code> followed by a VLAN ID (between 1 and 4094). For example, enter <code>mvr 2</code> to configure multicast settings on VLAN 2.	<code>sysname(config-mvr) #</code>
config-vdsl-alarmprofile	This is a sub-mode of the config mode and allows you to configure VDSL alarm profiles..	Type <code>vlan-alarmprofile</code> followed by a profile name. For example, <code>vdsl-alarmprofile test</code> .	<code>sysname(config-vdslalarmprofile) #</code>
config-vdsl-profile	This is a sub-mode of the config mode and allows you to configure VDSL profiles.	Type <code>vlan-profile</code> followed by a profile name. For example, <code>vdsl-profile standard</code> .	<code>sysname(config-vdslprofile) #</code>
Config-vlan	This is a sub-mode of the config mode and allows you to configure VLAN settings.	Type <code>vlan</code> followed by a number (between 1 and 4094). For example, <code>vlan 10</code> to configure settings for VLAN 10.	<code>sysname(config-vlan) #</code>

32.9 Using Command History

The switch keeps a list of command(s) you have entered for the current CLI session. You can use any commands in the history again by pressing the up (▲) or down (▼) arrow key to scroll through the previously used commands and press [ENTER]. Use the history command to display the list of commands.

```
sysname> history
  enable
  exit
  history
sysname>
```


32.10 Saving Your Configuration

After you set the switch settings with the configuration commands, use the `write memory` command to save the changes permanently.

```
sysname# write memory
```



The `write memory` command is not available in User mode. You must save your changes after each CLI session. All unsaved configuration changes are lost once you restart the switch.

32.10.1 Logging Out

In User or Enable mode, enter the `exit` or `logout` command to log out of the CLI. In Config mode entering `exit` takes you out of the Config mode and into Enable mode and entering `logout` logs you out of the CLI.

32.11 Command Summary

The following sections summarize the commands available in the switch together with a brief description of each command. Commands listed are in alphabetical order. The **P** column on the right indicates the administrator privilege level needed to use the command.

See the related section in the User's Guide for more background information.

32.11.1 User Mode

The following table describes the commands available for User mode.

Table 79 Command Summary: User Mode

COMMAND		DESCRIPTION	P
enable		Accesses Enable (or privileged) mode. See Section 32.11.2 on page 218 .	0
exit		Logs out from the CLI.	0
help		Displays help information.	0
history		Displays a list of previously command(s) that you have executed. The switch stores up to 256 commands in history.	0
logout		Exits from the CLI.	0
ping	<ip host-name> <[in-band out-of-band vlan <vlan-id>] [size <0-1472>] [-t]>	Sends Ping request to an Ethernet device.	0
	help	Displays command help information.	0

Table 79 Command Summary: User Mode (continued)

COMMAND		DESCRIPTION	P
show	hardware-monitor <C F>	Displays current hardware monitor information with the specified temperature unit (Celsius C or Fahrenheit F).	0
	hardware-version	Displays whether the Switch is a VDSL1 (100100 or 10050) or VDSL2 device (5030).	0
	ip	Displays the IP settings.	0
	system-information	Displays general system information.	0
ssh	<1 2> <[user@]dest-ip>	Connects to an SSH server with the specified SSH version.	0
traceroute	<ip host-name> [in-band out-of-band vlan <vlan-id>] [ttl <1-255>] [wait <1-60>] [queries <1-10>]	Determines the path a packet takes to a device.	0
	help	Displays the command help information.	0

32.11.2 Enable Mode

The following table describes the commands available for Enable mode.

Table 80 Command Summary: Enable Mode

COMMAND			DESCRIPTION	P
baudrate	<1 2 3 4 5>		Changes the console port speed. Choices are 1 (9600), 2 (19200), 3(38400), 4 (57600) and 5 (115200).	13
boot	config		Restarts the system.	13
configure			Accesses Configuration mode. See Section 32.11.3 on page 223 .	13
copy	running-config	tftp <ip> <remote-file>	Backs up running configuration to the specified TFTP server with the specified file name.	13
	tftp	config <index> <ip> <remote-file>	Restores configuration with the specified filename from the specified TFTP server.	13
		flash <ip> <remote-file>	Restores firmware via TFTP.	13
disable			Exits Enable (or privileged) mode.	13
enable			Accesses Enable (or privileged) mode.	13
erase	running-config		Resets to the factory default settings.	13
exit			Exits Enable (or privileged) mode.	13
help			Displays help information.	13
history			Displays a list of command(s) that you have previously executed.	13
igmp-flush			Clears all IGMP information.	13

Table 80 Command Summary: Enable Mode (continued)

COMMAND			DESCRIPTION	P
kick	tcp <session ID>		Disconnects the specified TCP session.	13
logout			Exits Enable (or privileged) mode.	13
mac-flush			Clears the MAC address table.	13
	<port-num>		Removes all learned MAC address on the specified port(s).	13
no	arp		Clears the ARP table.	13
	interface	<port-number>	Clears interface statistics.	13
	logging		Clears system logs.	13
ping	<ip host-name> [in-band out-of-band vlan <vlan-id>] [size <0-1472>] [-t]		Sends Ping request to an Ethernet device.	13
	help		Displays command help information.	13
reload	config		Restarts the system with the stored configurations.	13
show	classifier		Displays all classifier related information.	13
		<name>	Displays the specified classifier related information.	13
	cluster		Displays cluster management status.	13
		candidates	Displays cluster candidate information.	13
		member	Displays the MAC address of the cluster member(s).	13
		member config	Displays the configuration of the cluster member(s).	13
		member mac <mac-addr>	Displays the status of the cluster member(s).	13
	diffserv		Displays general DiffServ settings.	13
	garp		Displays GARP information.	13
	hardware-monitor <C F>		Displays current hardware monitor information with the specified temperature unit (Celsius C or Fahrenheit F).	13
	hardware-version		Displays whether the Switch is a VDSL1 (100100 or 10050) or VDSL2 device (5030).	13
	https		Displays the HTTPS information.	13
		certificate	Displays the HTTPS certificates.	13
		key <rsa dsa>	Displays the HTTPS key.	13
		session	Displays current HTTPS session(s).	13
		timeout	Displays the HTTPS session timeout.	13

Table 80 Command Summary: Enable Mode (continued)

COMMAND			DESCRIPTION	P
	igmp-filtering	profile	Displays IGMP filtering profile settings.	13
	igmp-snooping		Displays global IGMP snooping settings.	13
	interfaces <port-number>		Displays current interface status.	13
	interfaces config <port-list>		Displays current interface configuration.	13
		bandwidth-control	Displays bandwidth control settings.	13
		bstorm-control	Displays broadcast storm control settings.	13
		egress	Displays outgoing port information.	13
		igmp-filtering	Displays IGMP filtering settings.	13
		igmp-group-limited	Displays the IGMP group limit.	13
		igmp-immediate-leave	Displays the IGMP Immediate Leave setting.	13
		igmp-query-mode	Displays IGMP query mode settings.	13
		protocol-based-vlan	Displays protocol-based VLAN settings.	13
	ip		Displays IP related information.	13
		arp	Displays the ARP table.	13
		route	Displays IP routing information.	13
		route static	Displays IP static route information.	13
		tcp	Displays IP TCP status.	13
		udp	Displays UDP status.	13
	lACP		Displays LACP (Link Aggregation Control Protocol) settings.	13
	logging		Clears system logs.	13
	loginPrecedence		Displays login precedence settings.	13
	logins		Displays login account information.	13
	mac address-table	all <sort>	Displays MAC address table. sort = mac, vid or port.	13
		count	Displays the count of the MAC addresses stored in the MAC address table.	13
		static	Displays static MAC address table.	13
	mac-aging-time		Displays MAC learning aging time.	13
	multicast		Displays multicast settings.	13
	multi-login		Displays multi-login information	13
	mvr		Displays all MVR (Multicast VLAN Registration) settings.	13

Table 80 Command Summary: Enable Mode (continued)

COMMAND			DESCRIPTION	P
		<VID>	Displays the specified MVR group settings.	13
	plt		Displays Packet Loop Test (PLT).	13
	policy		Displays all policy related information.	13
		<name>	Displays the specified policy related information.	13
	port-access-authenticator		Displays all port authentication settings.	13
		<port-list>	Displays port authentication settings on the specified port(s).	13
	port-security		Displays all port security settings.	13
		<port-list>	Displays port security settings on the specified port(s).	13
	radius-server		Displays RADIUS server settings.	13
	remote-management		Displays all secured client information.	13
		<index>	Displays the specified secured client information.	13
	running-config		Displays current operating configuration.	13
	service-control		Displays service control settings.	13
	sfp	display	Displays detailed information of the SFP transceiver(s) installed in the mini GBIC slot(s).	13
	snmp-server		Displays SNMP settings.	13
	spanning-tree	config	Displays Spanning Tree Protocol (STP) settings.	13
	ssh		Displays general SSH settings.	13
		key <rsa1 rsa dsa>	Displays internal SSH public and private key information.	13
		known-hosts	Displays known SSH hosts information.	13
		session	Displays current SSH session(s).	13
	system-information		Displays general system information.	13
	time		Displays current system time and date.	13
	timesync		Displays time server information.	13
	trunk		Displays link aggregation information.	13
	vdsl-alarmprofile		Displays a summary list of VDSL alarm profiles.	13
		<profile-name>	Displays the settings of a VDSL alarm profile.	13
	vdsl-profile		Displays a summary list of VDSL profiles.	13

Table 80 Command Summary: Enable Mode (continued)

COMMAND			DESCRIPTION	P
		<profile-name>	Displays settings of the specified VDSL profile.	13
	vdsl-psdprofile		Displays a summary list of VDSL PSD profiles.	13
		<profile-name>	Displays settings of the specified VDSL PSD profile.	13
	vlan		Displays the status of all VLANs.	13
		<vlan-id>	Displays the status of the specified VLAN.	13
	vlan1q	gvrp	Displays GVRP settings.	13
		port-isolation	Displays VLAN-based port isolation settings.	13
	vlan-stacking		Displays VLAN stacking settings.	13
ssh	<1 2> <[user@]dest-ip>		Connects to an SSH server with the specified SSH version.	13
		<command </>>	Connects to an SSH server with the specified SSH version and addition commands to be executed on the server.	13
traceroute	<ip host-name>		Determines the path a packet takes to a device.	13
		[<vlan-id>] [ttl <1-255>] [wait <1-60>] [queries <1-10>]	Determines the path a packet takes to a device in the specified VLAN.	13
vdsl <port-list>	remote-reset		Resets the connection information and settings on the remote CPE device(s).	13
	remote-test		Sets the port(s) to test the connection to the remote CPE device(s).	13
	reset		Clears port statistics and connection information. This re-initializes the connection.	13
	retrain		Sets the port(s) to establish the connection again.	13
write	memory		Saves current configuration to the configuration file the switch is currently using.	13

32.11.3 General Configuration Mode

The following table lists the commands in Configuration (or Config) mode.

Table 81 Command Summary: Configuration Mode

COMMAND			DESCRIPTION	P
admin-password	<pw-string> <confirm-string>		Changes the administrator password.	14
bandwidth-control			Enables bandwidth control.	13
bcp-transparency			Enables Bridge Control Protocol (BCP) transparency.	13
classifier	<name> <[packet-format <802.3untag 802.3tag EtherIIuntag EtherIItag>][priority <0-7>][vlan <vlan-id>][ethernet-type <ethernet-num ip ipx arp rarp apple talk decnet sna netbios dlc][source-mac <src-mac-addr>][source-port <port-num>][destination-mac <dest-mac-addr>][dscp<0-63>][ip-protocol<protocol-num tcp udp icmp egp ospf rsvp igmp igp pim ipsec>][establish-only]][source-ip <src-ip-addr>[mask-bits <mask-bits>]][source-socket <socket-num>][destination-ip <dest-ip-addr> [mask-bits <mask-bits>]][destination-socket <socket-num>][inactive]>		Configures a classifier. A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming port number.	13
	help		Displays command information.	13
cluster	<vlan-id>		Sets the cluster management VLAN ID.	13
	member <mac-address>	password <password-str>	Sets the cluster member switch's hardware MAC address and password.	13
	name <cluster name>		Configures a name to identify the cluster manager.	13
	rcommand <mac-address>		Logs into a cluster member switch.	13
default-management	<in-band out-of-band>		Specifies through which traffic flow the switch is to send packets.	13
dhcp-relay			Enables DHCP relay settings.	13

Table 81 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	P
	helper-address <remote-dhcp-server1>	[remote-dhcp-server2] [remote-dhcp-server3]	Sets the IP addresses of up to 3 DHCP servers.	13
	information <string>		Specifies the agent information the device to add to DHCP requests.	13
	option		Sets the device to add DHCP relay agent information.	13
diffserv			Enables DiffServ.	13
	dscp <0-63> priority <0-7>		Sets the DSCP-to-IEEE 802.1q mappings.	13
exit			Exits from the CLI.	13
garp	join <100-65535> leave <msec> leaveall <msec>		Configures GARP time settings.	13
help			Displays help information.	13
history			Displays a list of previous command(s) that you have executed.	13
hostname	<name_string>		Sets the switch's name for identification purposes.	13
https	cert-regeneration <rsa dsa>		Re-generates a certificate.	13
	timeout <0-65535>		Sets how many seconds a management session (via the web configurator) can be left idle before the session times out.	13
igmp-filtering			Enables IGMP filtering.	13
	<profile name> start-address <ip> end-address <ip>		Sets the starting and ending IGMP addresses.	13
igmp-snooping			Enables IGMP snooping.	13
	8021p-priority <0 - 7>		Sets a priority level (0-7) to which the switch changes the priority in outgoing IGMP control packets.	13
	host-timeout <1 - 16711450>		Sets the host timeout value.	13
	leave-timeout <1 - 16711450>		Sets the leave timeout value	13
	unknown-multicast-frame <drop flooding>		Sets the action on unknown multicast frames received.	13
interface port-channel <port-list>			Enables a port or a list of ports for configuration. See Section 32.11.4 on page 233 for more details.	13
ip	address <ip> <mask>		Sets the management IP address and subnet mask.	13

Table 81 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	P
		default-gateway <ip>	Sets the default gateway's IP address.	13
	name-server	<ip>	Sets the IP address of a domain name server.	13
	route<ip> <mask> <next-hop-ip>		Creates a static route.	13
		[metric <metric>] [name <name>] [inactive]	Sets the metric of a static route or deactivates a static route.	13
lacp			Enables Link Aggregation Control Protocol (LACP).	13
	system-priority	<1-65535>	Sets the priority of an active port using LACP.	13
loginPrecedence	<LocalOnly LocalRADIUS RADIUSOnly>		Select which database the switch should use (first) to authenticate a user.	14
logins	username <name>	password <pwd>	Configures up to four read-only login accounts.	14
		privilege <0-14>	Sets the access privilege for the existing login accounts. The higher the value, the more commands are allowed.	14
logout			Exits from the CLI.	13
mac-aging-time	<10-3000>		Sets learned MAC aging time.	13
mac-filter	name <name> mac <mac-addr> vlan <vlan-id> drop <src/dst/both>		Configures a static MAC address port filtering rule.	13
		inactive	Disables a static MAC address port filtering rule.	13
mac-forward	name <name> mac <mac-addr> vlan <vlan-id> interface <interface-id>		Configures a static MAC address forwarding rule.	13
		inactive	Disables a static MAC address forwarding rule.	13
mirror-port			Enables port mirroring.	13
	<port-num>		Sets a monitor port.	13
mode	zynos		Changes the CLI mode to the ZyNOS format.	13
multi-login			Enables multi-login.	14
mvr <vlan-id>			Enters the MVR (Multicast VLAN Registration) configuration mode. See Section 32.11.5 on page 236 for more information.	13
no	bandwidth-control		Disable bandwidth control on the switch.	13

Table 81 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	P
	bcp-transparency		Disables Bridge Control Protocol (BCP) transparency.	13
	classifier <name>		Disables the classifier. Each classifier has one rule. If you disable a classifier you cannot use policy rule related information.	13
		inactive	Enables a classifier.	13
	cluster		Disables cluster management on the switch.	13
		member <mac-address>	Removes the cluster member.	13
	dhcp-relay		Disables DHCP relay.	13
		information	Disables the relay agent information option 82.	13
		option	System name is not appended to option 82 information field.	13
	diffserv		Disables the DiffServ settings.	13
	https	timeout	Resets the session timeout to the default of 300 seconds.	13
	igmp-filtering		Disables IGMP filtering on the switch.	13
		profile <name>	Disables the specified IGMP filtering profile.	13
		profile <name> start-address <ip> end-address <ip>	Clears the settings of the specified IGMP filtering profile.	13
	igmp-snooping		Disables IGMP snooping on the switch.	13
		8021p-priority	Disables 8021p-priority change in the outgoing IGMP control packets.	13
	ip		Disables management.	13
	ip route <ip> <mask>		Removes a specified IP static route.	13
		inactive	Enables a specified IP static route.	13
	lACP		Disables the link aggregation control protocol (dynamic trunking) on the switch.	13
	logins	username <name>	Disables login access for the specified account name.	14
	mac-filter name <name> mac <mac-addr> vlan <vlan-id>		Disables the specified MAC filter rule.	13
		inactive	Enables the specified MAC-filter rule.	13

Table 81 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	P
	mac-forward name <name> mac <mac-addr> vlan <vlan-id> interface <interface-id>		Removes the specified MAC forwarding entry, belonging to a VLAN group (if any) forwarded through an interface(s).	13
		inactive	Enables the specified MAC address, belonging to a VLAN group (if any) forwarded through an interface(s).	13
	mirror-port		Disables port mirroring on the switch.	13
	multi-login		Disables multiple logins.	14
	mvr <vlan-id>		Disable MVR on the switch.	13
	policy <name>		Deletes the specified policy. A policy sets actions for the classified traffic.	13
		inactive	Enables a policy.	13
	port-access-authenticator		Disables port authentication on the switch.	13
		<port-list>	Disables authentication on the listed ports.	13
		<port-list> reauthenticate	Disables the re-authentication mechanism on the listed port(s).	13
	port-security		Disables port security on the switch.	13
		<port-list>	Disables port security on the specified ports.	13
		<port-list> learn inactive	Enables MAC address learning on the specified ports.	13
	radius-server		Disables the use of authentication from the RADIUS server.	13
	remote-management <index>		Clears a secure client set entry from the list of secure clients.	13
		service <[telnet] [ftp] [http] [icmp] [snmp] [ssh] [https]>	Disables a secure client set entry number from using the selected remote management service(s).	13
	service-control	ftp	Disables FTP access to the switch.	13
		http	Disables web browser control to the switch.	13
		https	Disables secure web browser access to the switch.	13
		icmp	Disables ICMP access to the switch such as pinging and tracerouting.	13
		snmp	Disables SNMP management.	13

Table 81 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	P
		ssh	Disables SSH (Secure Shell) server access to the switch.	13
		telnet	Disables telnet access to the switch.	13
	snmp-server	trap-destination <ip>	Disables sending of SNMP traps to a station.	13
	spanning-tree		Disables (R)STP.	13
		<port-list>	Disables (R)STP on the specified ports.	13
	ssh	key <rsa rsa dsa>	Disables the secure shell server encryption key. Your switch supports SSH versions 1 and 2 using RSA and DSA authentication.	13
		known-hosts	Removes all remote hosts.	13
		known-hosts <host-ip>	Removes the specified remote hosts from the list of all known hosts.	13
		known-hosts <host-ip> [1024 ssh-rsa ssh-dsa]	Removes remote known hosts with the specified public key (1024-bit RSA1, RSA or DSA).	13
	storm-control		Disables broadcast storm control.	13
	syslog		Disables syslog logging.	13
		server <ip-address>	Disables syslog logging to the specified syslog server.	13
		server <ip-address> inactive	Enables syslog logging to the specified syslog server.	13
		type <type>	Disables syslog logging for the specified log type (sys, link, config, error or report).	13
	timesync		Removes the time server protocol.	13
	trunk <Tl>		Disables port group trunking.	13
		interface <port-list>	Removes ports from the trunk group.	13
		lACP	Disables LACP in the trunk group.	13
	vds1-alarmprofile	<profile-name>	Removes a VDSL alarm profile. You cannot delete a default profile (DEFVAL).	13
	vds1-profile	<profile-name>	Removes a VDSL profile. You cannot delete a default profile (DEFVAL).	13
	vds1-psd profile	<profile-name>	Removes a VDSL PSD profile. You cannot delete a default profile (DEFVAL).	13

Table 81 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	P
		<profile-name> physide <1 2> frequency <0 - 30000>	Removes the specified breakpoint in a VDSL PSD profile.	13
	vlan	<vlan-id>	Deletes the static VLAN entry.	13
	vlanlq	gvrp	Disables GVRP on the switch.	13
		port-isolation	Disables port isolation.	13
	vlan-stacking		Disables VLAN stacking.	13
	wfq fe-spq		Disables Strict Priority Queuing on the fast Ethernet (10/100Mbps) ports.	13
password	<password>		Change the password for Enable mode.	14
policy	<name> classifier <classifier-list> <[vlan<vlan-id>] [egress-port <port-num>] [priority <0-7>] [dscp <0-63>] [tos <0-7>] [bandwidth <bandwidth>] [egress-mask<port-list>] [outgoing-packet-format <tagged untagged>] [out-of-profile-dscp <0-63>] [forward-action <drop forward egressmask>] [queue-action <prio-set prio-queue prio-replace-tos>] [diffserv-action <diff-set-tos diff-replace-priority diff-set-dscp>] [outgoing-mirror] [outgoing-eport] [outgoing-non-unicast-eport] [outgoing-set-vlan] [metering] [out-of-profile-action<[change-dscp] [drop] [forward] [set-drop-prec] [inactive]>]		Configures a policy. A classifier distinguishes traffic into flows based on the configured criteria. A policy rule ensures that a traffic flow gets the requested treatment in the network.	13
	help		Displays command information.	13
port-access-authenticator			Enables 802.1x authentication on the switch.	13
	<port-list>		Enables 802.1x authentication on the specified port(s).	13

Table 81 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	P
		reauthenticate	Sets a subscriber to periodically re-enter his or her username and password to stay connected to a specified port.	13
		reauth-period <reauth-period>	Specifies how often a client has to re-enter the username and password to stay connected to the specified port(s).	13
port-security			Enables port security on the switch.	13
	<port-list>		Enables the port security feature on the specified port(s).	13
		address-limit <number>	Disables MAC address learning on the specified port(s).	13
		learn inactive	Limits the number of (dynamic) MAC addresses that may be learned on a port.	13
		MAC-freeze	Disables MAC address learning and enables port security. Note: All previously learned dynamic MAC addresses are saved to the static MAC address table.	13
queue	level <0-7> priority <0-7>		Sets the priority level-to-physical queue mapping.	13
radius-server	host <ip>		Sets the IP address of the external RADIUS server.	13
		[acct-port <socket-number>] [key <key-string>]	Sets the UDP port and shared key for the external RADIUS server.	13
remote-management	<index>		Enables a remote management setting.	13
		start-addr <ip> end-addr <ip> service <[telnet] [ftp] [http] [icmp] [snmp] [ssh] [https]>	Specifies a group of trusted computer(s) from which an administrator may use a service to manage the switch.	13
service-control	ftp <socket-number>		Allows FTP access on the specified service port.	13
	http <socket-number> <timeout>		Allows HTTP access on the specified service port and defines the timeout period.	13

Table 81 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	P
	https <socket-number>		Allows HTTPS access on the specified service port.	13
	icmp		Allows ICMP access for services like Ping.	13
	snmp		Allows SNMP management.	13
	ssh <socket-number>		Allows SSH access on the specified service port.	13
	telnet <socket-number>		Allows Telnet access on the specified service port.	13
snmp-server	[contact <system contact>] [location <system location>]		Sets the geographic location and the name of the person in charge of this switch.	13
	get-community <property>		Sets the get community.	13
	set-community <property>		Sets the set community.	13
	trap-community <property>		Sets the trap community.	13
	trap-destination <ip>		Sets the IP addresses of up to four stations to send your SNMP traps to.	13
spanning-tree			Enables STP on the switch.	13
	<port-list>		Enables STP on a specified port.	13
	<port-list> path-cost <1-65535>		Sets the STP path cost for a specified port.	13
	<port-list> priority <0-255>		Sets the priority for a specified port.	13
	hello-time <1-10> maximum-age <6-40> forward-delay <4-30>		Sets Hello Time, Maximum Age and Forward Delay.	13
	help		Displays command help information.	13
	priority <0-61440>		Sets the bridge priority of the switch.	13
spq			Sets the switch to use Strictly Priority Queuing (SPQ).	13
ssh	known-hosts <host-ip> <1024 ssh-rsa ssh-dsa> <key>		Adds a remote host to which the switch can access using SSH service.	13
storm-control			Enables broadcast storm control on the switch.	13
syslog			Enables syslog logging.	13
	server <ip-adderss>	inactive	Disables syslog logging to the specified syslog server.	13
		level <0 ~ 7>	Sets the IP address of the syslog server and the severity level.	13

Table 81 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	P
	type <type>		Sets the log type.	13
		facility <0 ~ 7>	Sets the log type and the file location on the syslog server.	13
time	<Hour:Min:Sec>		Sets the time in hour, minute and second format.	13
	date <month/day/year>		Sets the date in year, month and day format.	13
	help		Displays help information.	13
	timezone <-1200 ... 1200>		Selects the time difference between UTC (formerly known as GMT) and your time zone.	13
timesync	<daytime time ntp>		Sets the time server protocol.	13
	server <ip>		Sets the IP address of your time server.	13
trunk	<T1>		Activates port group trunking.	13
		interface <port-list>	Adds a port(s) to the trunk group.	13
		lacp	Enables LACP for the trunk group.	13
	interface <port-list>	timeout <lacp-timeout>	Defines the port number and LACP timeout period.	13
vdsl-alarmprofile <name>			Enters the VDSL alarm profile mode. See Section 32.11.6 on page 237 for more information.	13
vdsl-port	<port-list>	<enable disable>	Activates/deactivates the VDSL port(s).	13
		alarm-profilename <name-str>	Sets the VDSL port(s) to use the VDSL alarm profile.	13
		profilename <name-str>	Sets the VDSL port(s) to use the VDSL profile.	13
		psd-profilename <name-str>	Sets the VDSL port(s) to use the VDSL PSD profile.	13
vdsl-profile <name>			Enters VDSL profile command mode. See Section 32.11.7 on page 238 for more information.	13
vdsl-psd profile <name>	physide <1 2> frequence <0 - 30000> level <125 - 1400>		Sets a VDSL PSD profile. 1: DownStream 2: UpStream	13
vlan	<1-4094>		Enters the VLAN configuration mode. See Section 32.11.8 on page 240 for more information.	13
vlan1q	gvrp		Enables GVRP.	13
	port-isolation		Enables VLAN port isolation on all ports.	13

Table 81 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	P
vlan-stacking			Enables VLAN stacking on the device.	13
	<SPTPID>		Sets the service provider's TP (Tagged Protocol) ID.	13
vlan-type	<802.1q port-based>		Specifies the VLAN type.	13
wfq			Sets the switch to use Weight Fair Queuing (WFQ) queuing.	13
	fe-spq <Q0-Q7>		Sets the switch to use WFQ to service all queues for the Ethernet port.	13

32.11.4 interface Commands

The following table lists the `interface port-channel` commands in configuration mode. Use these commands to configure the ports.

Table 82 interface port-channel Commands

COMMAND			DESCRIPTION	P
interface port-channel <port-list>			Enables a port or a list of ports for configuration.	13
	bandwidth-limit		Enables bandwidth control on the port(s).	13
		cir <Kbps>	Sets the guaranteed bandwidth allowed for incoming traffic on the port(s).	13
		egress <Kbps>	Sets the maximum bandwidth allowed for outgoing traffic on the port(s).	13
		pir <Kbps>	Sets the maximum bandwidth allowed for incoming traffic on the port(s).	13
	bpdu-control <peer tunnel discard network>		Sets how Bridge Protocol Data Units (BPDUs) are used in STP port states.	13
	broadcast-limit		Enables broadcast storm control limit on the switch.	13
		<pkt/s>	Sets how many broadcast packets the interface receives per second.	13
	cable_diagnostics		Displays whether a cable is connected to the port (good) or not (open).	13
	diffserv		Enables DiffServ settings on the port(s).	13
	dlf-limit		Enables the Destination Lookup Failure (DLF) limit.	13
		<pkt/s>	Sets the interface DLF limit in packets per second (pps).	13
	egress set <port-list>		Sets the outgoing traffic port list for a port-based VLAN.	13

Table 82 interface port-channel Commands (continued)

COMMAND			DESCRIPTION	P
	exit		Exits from the interface port-channel command mode.	13
	flow-control		Enables interface flow control. Flow control regulates transmissions to match the bandwidth of the receiving port.	13
	frame-type <all tagged untagged>		Choose to accept both tagged and untagged incoming frames or just tagged incoming frames on a port.	13
	gvrp		Enables this function to permit VLAN groups beyond the local switch.	13
	help		Displays a description of the interface port-channel commands.	13
	igmp-filtering	profile <name>	Applies the specified IGMP filtering profile.	13
	igmp-group-limit		Enables the IGMP group limiting feature.	13
		number <number>	Sets the maximum number IGMP groups allowed.	13
	igmp-immediate-leave		Enables the IGMP immediate leave function.	13
	igmp-querier-mode <auto fixed edge>		Sets the IGMP querier mode of a port. <i>auto</i> uses the port as an IGMP query port after it receives IGMP query packets. <i>fixed</i> always uses the port as an IGMP query port. <i>edge</i> stops the switch from using the port as an IGMP query port.	13
	inactive		Disables the specified port(s) on the switch.	13
	ingress-check		Enables the device to discard incoming frames for VLANs that are not included in a port member set.	13
	intrusion-lock		Enables intrusion lock on a port and a port cannot be connected again after you disconnected the cable.	13
	mirror		Enables port mirroring on the port(s).	13
		dir <ingress egress both>	Enables port mirroring for incoming, outgoing or both incoming and outgoing traffic. Port mirroring copies traffic from one or all ports to another or all ports for external analysis.	13
	multicast-limit		Enables the port(s) multicast limit.	13
		<pkt/s>	Sets how many multicast packets the port(s) receives per second.	13
	name <port-name-string>		Sets a name for the port(s). Enter a descriptive name (up to nine printable ASCII characters).	13

Table 82 interface port-channel Commands (continued)

COMMAND			DESCRIPTION	P
	no	bandwidth-limit	Disables bandwidth limit on the port(s).	13
		broadcast-limit	Disables broadcast storm control limit on the port(s).	13
		diffserv	Disables DiffServ settings on the port(s).	13
		dlf-limit	Disables destination lookup failure (DLF) on the switch.	13
		egress set <port-list>	Sets the outgoing traffic port list for a port-based VLAN.	13
		flow-control	Disables flow control on the port(s).	13
		gvrp	Disable GVRP on the port(s).	13
		igmp-filtering profile	Disables IGMP filtering.	13
		igmp-group-limit	Disables IGMP group limitation.	13
		igmp-immediate-leave	Disables the IGMP immediate leave function.	13
		inactive	Enables the port(s) on the switch.	13
		ingress-check	Disables ingress checking on the port(s).	13
		intrusion-lock	Disables intrusion-lock on a port so that a port can be connected again after you disconnected the cable.	13
		mirror	Disables port mirroring on the port(s).	13
		multicast-limit	Disables multicast limit on the port(s).	13
		protocol-based-vlan ethernet-type <ethe>	Disables protocol based VLAN of the specified protocol on the port(s).	13
		protocol-based-vlan packet-format <pack> ethernet-type <ethernet-type>	Disables protocol based VLAN of the specified packet format on the port(s).	13
		vlan-trunking	Disables VLAN trunking on the port(s).	13
	protocol-based-vlan name <name>	ethernet-type <ethernet-type> vlan <vid>	Creates a protocol based VLAN with the protocol type and VLAN ID.	13
		ethernet-type <ethernet-type> vlan <vid> inactive	Disables the protocol based VLAN.	13
		packet-format <packet-format> ethernet-type <ethernet-type> vlan <vid> priority <0-7>	Creates a protocol based VLAN with the packet format, VLAN ID and priority.	13

Table 82 interface port-channel Commands (continued)

COMMAND			DESCRIPTION	P
		packet-format <packet-format> ethernet-type <ethernet-type> vlan <vid> priority <0-7> inactive	Disables the protocol based VLAN.	13
	pvid <1-4094>		The default PVID is VLAN 1 for all ports. Sets a PVID in the range 1 to 4094 for the specified interface.	13
	qos priority	<0-7>	Sets the quality of service priority for an interface.	13
	speed-duplex	<auto 10-half 10-full 100-half 100-full 1000-full>	Sets the duplex mode (half or full) and speed (10, 100 or 1000 Mbps) of the connection on the interface. Selecting auto (auto-negotiation) makes one port able to negotiate with a peer automatically to obtain the connection speed and duplex mode that both ends support.	13
	test		Performs an interface loopback test.	13
	vlan-stacking	priority <0-7>	Sets the priority of the specified port(s) in VLAN stacking.	13
		role <normal access tunnel>	Sets the VLAN stacking port roles of the specified port(s).	13
		SPVID <1-4094>	Sets the service provider VID of the specified port(s).	13
	vlan-trunking		Enables VLAN Trunking on ports connected to other switches or routers (but not ports directly connected to end users) to allow frames belonging to unknown VLAN groups to pass through the switch.	13
	weight <wt1> <wt2> ... <wt8>		Sets the queuing weight.	13

32.11.5 mvr Commands

The following table lists the `mvr` commands in configuration mode.

Table 83 mvr Commands

COMMAND			DESCRIPTION	P
mvr <1-4094>			Enters the MVR (Multicast VLAN Registration) configuration mode.	13
	8021p-priority <0 - 7>		Select a priority level (0-7) with which the switch replaces the priority in outgoing IGMP control packets (belonging to this multicast VLAN).	13
	exit		Exist from the MVR configuration mode.	13

Table 83 mvr Commands (continued)

COMMAND			DESCRIPTION	P
	group <name-str> start-address <ip> end-address <ip>		Sets the multicast group range for the MVR.	13
	inactive		Disables MVR settings.	13
	mode <dynamic compatible>		Sets the MVR mode.	13
	name <name>		Sets the MVR name for identification purposes.	13
	no	group	Disables all MVR group settings.	13
		group <name>	Disables the specified MVR group setting.	13
		inactive	Enables MVR.	13
		receiver-port <port-list>	Disables the receiver port(s). An MVR receiver port can only receive multicast traffic in a multicast VLAN	13
		source-port <port-list>	Disables the source port(s). An MVR source port can send and receive multicast traffic in a multicast VLAN	13
		tagged <port-list>	Sets the port(s) to remove VLAN tags.	13
	receiver-port <port-list>		Sets the receiver port(s). An MVR receiver port can only receive multicast traffic in a multicast VLAN	13
	source-port <port-list>		Sets the source port(s). An MVR source port can send and receive multicast traffic in a multicast VLAN	13
	tagged <port-list>		Sets the port(s) to include VLAN tags.	13

32.11.6 vdsl-alarmprofile Commands

The following table lists the vdsl-alarmprofile commands in configuration mode.

Table 84 vdsl-alarmprofile Commands

COMMAND			DESCRIPTION	P
vdsl-alarmprofile <name>			Enters the VDSL alarm profile mode.	13
	15minsESs <threshold>		Sets the number of Errored Seconds (ES) allowed in any 15-minute period. An alarm is triggered if this number is exceeded.	13

Table 84 vdsl-alarmprofile Commands (continued)

COMMAND		DESCRIPTION	P
	15minsLoss <threshold>	Sets the number of Lost of Signal (Los) errors allowed in any 15-minute period. An alarm is triggered if this number is exceeded.	13
	15minsSESS <threshold>	Sets the number of Severely Errored Seconds(SES) errors allowed in any 15-minute period. An alarm is triggered if this number is exceeded.	13
	exit	Exits from this command mode.	13
	initFailure <on off>	Sets whether the device is to send an initialization failure trap or not.	13

32.11.7 vdsl-profile Commands

The following table lists the vdsl-profile commands in configuration mode.

Table 85 vdsl-profile Commands

COMMAND		DESCRIPTION	P
vdsl-profile <name>		Enters VDSL profile command mode.	13
	applicablestandard <2>	Sets a standard your switch uses for VDSL services. 2: ETSI	13
	bandplan <2>	Sets a VDSL band plan to use for the line. 2: Bandplan998	13
	compatiblemode <1..4>	Sets the starting band of the frequency range used by VDSL services. 1: none 2: 640kHz 3: 1100kHz 4: 2200kHz	13
	deployment <1..2>	Specify a VDSL deployment scenario. 1: FTTCab 2: FTTEEx	13
	exit	Exits from the VDSL profile mode.	13
	hamband	mask <000000000000..0000111100>	13
	interleavedelay	ds <0..255>	13
		us <0..255>	13

Table 85 vdsl-profile Commands (continued)

COMMAND			DESCRIPTION	P
	maxpower	ds <0..58>	Specify the maximum aggregate power level for downstream transmission.	13
		us <0..58>	Specify the maximum aggregate power level for upstream transmission.	13
	optusage <1..2>		Sets the use of optional channel for the upstream or downstream traffic. 1: unused 2: upstream	13
	payloadrate	maxdsfast <64..104960>	Specifies the maximum downstream fast channel data rate in bits/second.	13
		maxdsslow <64..104960>	Specifies the maximum downstream slow channel data rate in bits/second.	13
		maxusfast <64..104960>	Specifies the maximum upstream fast channel data rate in bits/second.	13
		maxusslow <64..104960>	Specifies the maximum upstream slow channel data rate in bits/second.	13
		mindsfast <64..104960>	Specifies the minimum downstream fast channel data rate in bits/second.	13
		mindsslow <64..104960>	Specifies the minimum downstream slow channel data rate in bits/second.	13
		minusfast <64..104960>	Specifies the minimum upstream fast channel data rate in bits/second.	13
		minusslow <64..104960>	Specifies the minimum upstream slow channel data rate in bits/second.	13
	pbo	uscontrol <1..3>	Sets the upstream PBO control. 1: Disable 2: Auto 3: Manual	13
		uslevel <0..120>	Sets the upstream PBO level.	13
	psdtemplate	ds <1..2>	Sets a PSD mask for the downstream traffic.	13
		us <1..2>	Sets a PSD mask for the upstream traffic.	13
	ratemode	ds <1 2>	Sets a rate adaptive mode for the downstream traffic 1: Manual 2: AdaptAtInit	13

Table 85 vdsl-profile Commands (continued)

COMMAND			DESCRIPTION	P
		us <1 2>	Sets a rate adaptive mode for the upstream traffic 1: Manual 2: AdaptAtInit	13
	rateratio	ds <0..100>	Specify the downstream data rate allocated for the fast and slow channels. 0: slow channel 100: fast channel	13
		us <0..100>	Specify the upstream data rate allocated for the fast and slow channels. 0: slow channel 100: fast channel	13
	snr	dsmax <0..127>	Sets the maximum downstream SNR (Signal to Noise Ratio).	13
		dsmin <0..127>	Sets the minimum downstream SNR (Signal to Noise Ratio).	13
		dstarget <0..127>	Sets the target downstream SNR (Signal to Noise Ratio).	13
		usmax <0..127>	Sets the maximum upstream SNR (Signal to Noise Ratio).	13
		usmin <0..127>	Sets the minimum upstream SNR (Signal to Noise Ratio).	13
		ustarget <0..127>	Sets the target upstream SNR (Signal to Noise Ratio).	13
	targetslowburst	ds <0..1275>	Sets the target burst rate for the downstream slow channel.	13
		us <0..1275>	Sets the target burst rate for the upstream slow channel.	13

32.11.8 vlan Commands

The following table lists the `vlan` commands in configuration mode.

Table 86 vlan Commands

COMMAND			DESCRIPTION	P
vlan <1-4094>			Creates a new VLAN group.	13
	exit		Leaves the VLAN configuration mode.	13
	fixed <port-list>		Specifies the port(s) to be a permanent member of this VLAN group.	13
	forbidden <port-list>		Specifies the port(s) you want to prohibit from joining this VLAN group.	13
	help		Displays a list of available VLAN commands.	13
	inactive		Disables the specified VLAN.	13
	ip address	<ip-address> <mask>	Sets the IP address and subnet mask of the switch in the specified VLAN for packet loopback test.	13

Table 86 vlan Commands (continued)

COMMAND			DESCRIPTION	P
		<ip-address> <mask> manageable	Allows the switch to be managed using this specified IP address.	13
		default-gateway <ip-address>	Sets a default gateway IP address for this VLAN.	13
		inband-default <ip-address> <mask>	Sets a static in-band IP address and subnet mask.	13
		inband-default dhcp-bootp <cr>	Sets the dynamic in-band IP address.	13
		inband-default dhcp-bootp release	Releases the dynamic in-band IP address.	13
		inband-default dhcp-bootp renew	Updates the dynamic in-band IP address.	13
	name <name-str>		Specifies a name for identification purposes.	13
	no	fixed <port-list>	Sets fixed port(s) to normal port(s).	13
		forbidden <port-list>	Sets forbidden port(s) to normal port(s).	13
		inactive	Enables the specified VLAN.	13
		ip address <ip-address> <mask>	Deletes the IP address and subnet mask in this VLAN.	13
		ip address default-gateway	Deletes the default gateway in this VLAN.	13
		ip address inband-default dhcp-bootp	Sets the default in-band interface to use a static IP address in this VLAN. The switch will use the default IP address of 0.0.0.0 if you do not configure a static IP address.	13
		untagged <port-list>	Specifies the port(s) you want to tag all outgoing frames transmitted with this VLAN Group ID.	13
	normal <port-list>		Specifies the port(s) to dynamically join this VLAN group using GVRP	13
	untagged <port-list>		Specifies the port(s) you don't want to tag all outgoing frames transmitted with this VLAN Group ID.	13

Command Examples

This chapter describes some commands in more detail.

33.1 Overview

These are commands that you may use frequently in maintaining your switch.

33.2 show Commands

These are the commonly used `show` commands.

33.2.1 show interface

Syntax:

```
show interface [port-number]
```

This command displays statistics of a port. The following example shows that port 2 is up and the related information.

```
sysname# show interface 2
Port Info      Port NO.      :2
               Link          :100M/F
               Status        :FORWARDING
               LACP          :Disabled
               TxPkts        :0
----- [Snip] -----
               LPRs          :0 / 0
               C15MinTimeElapsed :0 / 0
               Curr15MinLofs    :0 / 0
               Curr15MinLoss    :0 / 0
               Curr15MinLols    :0 / 0
               Curr15MinLprs    :0 / 0
               C1DayTimeElapsed :0 / 1
               Curr1DayLofs     :1 / 0
               Curr1DayLoss     :0 / 0
               Curr1DayLols     :0 / 0
               Curr1DayLprs     :0 / 0
sysname#
```

33.2.2 show ip

Syntax:

```
show ip
```

This command displays the IP related information (such as IP address and subnet mask) on all switch interfaces.

The following figure shows the default interface settings.

```
sysname> show ip
Out-of-band Management IP Address = 192.168.0.1
Management IP Address
    IP[192.168.0.1], Netmask[255.255.255.0], VID[0]
IP Interface
    IP[192.168.1.1], Netmask[255.255.255.0], VID[1]
```

33.2.3 show logging

Syntax:

```
show logging
```

This command displays the system logs. The following figure shows an example.

```
sysname# show logging
56 Thu Jan  1 00:01:04 1970 PSSV -WARN  SNMP TRAP 0: cold start
57 Thu Jan  1 00:01:04 1970 PSSV  WARN  System cold start
58 Thu Jan  1 00:01:04 1970 PP1f -WARN  SNMP TRAP 26: Event On Trap
59 Thu Jan  1 00:01:06 1970 PKEB  INFO  User admin login
60 Thu Jan  1 00:02:46 1970 PP0c -WARN  SNMP TRAP 3: port 18 link up
61 Thu Jan  1 00:02:46 1970 PP0c  ERROR Port 18 link up
62 Thu Jan  1 00:03:23 1970 PP27  INFO  User admin logout
63 Thu Jan  1 00:03:28 1970 PKEB  INFO  User admin login
Clear Error Log (y/n):
```

If you clear a log (by entering **y** at the Clear Error Log (y/n) :prompt), you cannot view it again.

33.2.4 show mac address-table all

Syntax:

```
show mac address-table all <sort>
```

Where

<sort> = Specifies the sorting criteria (MAC, VID or port).

This command displays the MAC address(es) stored in the switch. The following example shows the MAC address table.

```
sysname# show mac address-table all
Port      VLAN ID    MAC Address      Type
18         1          00:02:e3:30:43:34 Dynamic
18         1          00:04:80:9b:78:00 Dynamic
18         1          00:0d:60:8f:09:a1 Dynamic
18         1          00:0f:fe:1e:4a:e0 Dynamic
18         1          00:13:49:22:a3:3b Dynamic
18         1          00:c0:9f:cd:cc:5f Dynamic
18         1          00:c0:a8:fa:e9:27 Dynamic
sysname#
```

33.2.5 show multi-login

Syntax:

```
show multi-login
```

This command displays the multiple login settings or the number of CLI management sessions.

The following example shows that there are currently one console port and one Telnet sessions to the switch.

```
sysname# show multi-login
[session info ('*' denotes your session)]
index session    remote ip
-----
*  1 console      -
   2 telnet-d     172.23.37.10
sysname#
```

If the multiple login feature is disabled (using the `no multi-login` command in Config mode), the screen displays as shown.

```
sysname# show multi-login
multi-login is disabled
sysname#
```

33.2.6 show system-information

Syntax:

```
show system-information
```

This command shows the general system information (such as the firmware version and system up time). An example is shown next.

```
sysname# show system-information

System Name           : VES-1616F-35
System Contact        :
System Location       :
Ethernet Address      : 00:13:49:00:00:02
ZyNOS F/W Version     : V3.60 (AIH.0)C0 | 01/25/2007
RomRasSize            : 3364912
System up Time        :      0:28:28 (29b44 ticks)
Bootbase Version      : V0.1 | 06/05/2006
ZyNOS CODE            : RAS Jan 19 2007 19:22:28
Product Model         : VES-1616F-35
sysname#
```

33.2.7 show vdsl-alarmprofile

Syntax:

```
show vdsl-alarmprofile [<profile-name>]
```

This command displays a summary list of VDSL alarm profiles or displays the settings of a VDSL alarm profile. The following example shows the summary table.

```
sysname# show vdsl-alarmprofile

Name                               LOSs   ESs    SESs   InitFailure   Applied Ports
=====
DEFVAL                             0      0      0       Off           1-16
sysname#
```

The following example shows the settings of the test alarm profile.

```
sysname# show vdsl-alarmprofile test

Profile Name           : test
15Mins LOSs Threshold  : 15
15Mins ESs Threshold   : 10
15Mins SESs Threshold  : 5
Initialization Failure : On
sysname#
```

33.2.8 show vdsl-profile

Syntax:

```
show vdsl-profile [<profile-name>]
```

This command displays a summary list of VDSL profiles or displays the settings of a VDSL profile. The following example shows the summary table.

```
sysname# show vdsl-profile
```

Name	Payload Rate	SNR Margin	Applied Ports
DEFVAL	104M/104M	6/6	1-16
test	104M/104M	6/6	

```
sysname#
```

The following example shows the settings of the test VDSL profile.

```
sysname# show vdsl-profile test
```

```
Profile Name: test
```

	Downstream	Upstream
Slow Channel Payload Rate	MAX: 104960 MIN: 64	MAX: 104960 MIN: 64
Fast Channel Payload Rate	MAX: 104960 MIN: 64	MAX: 104960 MIN: 64
Rate Adaption	adaptAtInit	adaptAtInit
Max SNR Margin	31dB	31dB
Target SNR Margin	6dB	6dB
Min SNR Margin	0dB	0dB
Max Interleave Delay	2ms	2ms
Max Aggregate Power	14dBm	14dBm
Rate Raio	0%	0%
Impulse Noise Protection	0ms	0ms
FEC Redundancy	0%	0%
PSD Template Mask	templateMask2	templateMask2
PBO Control	disabled	disabled
PBO Level	0dB	0dB
Band Plan	bandPlan998	
Deployment Scenario	fttEx	
Compatible Mode	none	
Applicable Standard	etsi	
Ham Band Mask		
Custom Notch1 Start	0kHz	
Custom Notch1 Stop	0kHz	
Custom Notch2 Start	0kHz	
Custom Notch2 Stop	0kHz	
Optional Band	unused	
Line Type	fastOrInterleaved	

```
sysname#
```

33.3 ping

Syntax:

```
ping <ip> < [in-band|out-of-band|vlan <vlan-id> ] [ size <0-8024> ] [ -t ]>
```

where

<code><ip></code>	=	The IP address of an Ethernet device.
<code>[in-band out-of-band vlan <vlan-id>]</code>	=	Specifies the network interface or the VLAN ID to which the Ethernet device belongs. <code>out-of-band</code> refers the management port while <code>in-band</code> means the other ports on the switch.
<code>[size <0-8024>]</code>	=	Specifies the packet size to send.
<code>[-t]</code>	=	Sends Ping packets to the Ethernet device indefinitely. Click [CTRL]+ C to terminate the Ping process.

This command sends Ping packets to an Ethernet device. The following example sends Ping requests to and displays the replies from an Ethernet device with an IP address of 192.168.1.100.

```
sysname# ping 192.168.1.100
sent  rcvd  rate    rtt      avg      mdev      max      min  reply from
   1     1   100      0        0         0         0         0  192.168.1.100
   2     2   100      0        0         0         0         0  192.168.1.100
   3     3   100      0        0         0         0         0  192.168.1.100
sysname#
```

33.4 traceroute

Syntax:

```
traceroute <ip> [in-band|out-of-band|vlan <vlan-id>][ttl <1-255>] [wait <1-60>] [queries <1-10>]
```

where

<code><ip></code>	=	The IP address of an Ethernet device.
<code>[in-band out-of-band vlan <vlan-id>]</code>	=	Specifies the network interface or the VLAN ID to which the Ethernet device belongs.
<code>[ttl <1-255>]</code>	=	Specifies the Time To Live (TTL) period.
<code>[wait <1-60>]</code>	=	Specifies the time period to wait.
<code>[quesries <1-10>]</code>	=	Specifies how many tries the switch performs the traceroute function.

This command displays information about the route to an Ethernet device. The following example displays route information to an Ethernet device with an IP address of 192.168.1.100.

```
sysname> traceroute 192.168.1.100
traceroute to 192.168.1.100, 30 hops max, 40 byte packet
 1:192.168.1.100 (10 ms) (10 ms) (0 ms)
traceroute done:
```

33.5 Enabling RSTP

Syntax:

```
spanning-tree [port-number]
```

To enable RSTP on a port. Enter `spanning-tree` followed by the port number and press [ENTER]. The following example enables RSTP on port 17.

```
sysname(config)# spanning-tree 17
sysname#
```

33.6 vdsl-port Command

Syntax:

```
vdsl-port <port-list> profilename <name-str>
```

where

<port-list>	=	Selects the VDSL port(s) (port 1 to 16).
<name-str>	=	Specifies the name of the VDSL profile.

This command sets the specified VDSL port(s) to use a VDSL profile. The following example configures VDSL ports 1 to 5 to use the `test` VDSL profile.

```
sysname(config)# vdsl-port 1-5 profilename test
```

33.7 Configuration File Maintenance

This section shows you how to backup or restore the configuration file on the switch using TFTP.

33.7.1 Backing up Configuration

Syntax:

```
copy running-config tftp <ip> <remote-file>
```

where

- <ip> = The IP address of a TFTP server on which you want to store the backup configuration file.
- <remote-file> = Specifies the name of the configuration file.

This command backs up the current configuration file on a TFTP server. The following example backs up the current configuration to a file (`test.cfg`) on the TFTP server (172.23.19.96).

```
sysname# copy running-config tftp 172.23.19.96 test.cfg
Backupping
. (683)Bytes Done!
sysname#
```

33.7.2 Restoring Configuration

Syntax:

```
copy tftp config <index> <ip> <remote-file>
```

where

- <index> = Specifies to restore which configuration file (1) on the Switch.
- <ip> = The IP address of a TFTP server from which you want to get the backup configuration file.
- <remote-file> = Specified the name of the configuration file.

This command restores a configuration file on the switch. The following example uploads the configuration file (`test.cfg`) from the TFTP server (172.23.19.96) to the switch.

```
sysname# copy tftp config 1 172.23.19.96 test.cfg
Restoring
. (683)Bytes Done!
sysname#
```

33.7.3 Resetting to the Factory Default

Follow the steps below to reset the switch back to the factory defaults.

- 1 Enter `erase running-config` to reset the current running configuration.
- 2 Enter `write memory` to save the changes to the current configuration file.

The following example resets both configuration files to the factory default settings.

```
sysname# erase running-config
sysname# write memory
```

33.8 no Command Examples

These are the commonly used command examples that belong to the `no` group of commands.

33.8.1 no mirror port

Syntax:

```
no mirror-port
```

Disables port mirroring on the switch.

An example is shown next.

```
sysname(config)# no mirror-port
```

33.8.2 no https timeout

Syntax:

```
no https timeout
```

Resets the https session timeout to default.

An example is shown next. The session timeout is reset to 300 seconds.

```
sysname(config)# no https timeout
Cache timeout 300
```

33.8.3 no trunk

Syntax:

```
no trunk <T1>
no trunk <T1> lacp
no trunk <T1> interface <port-list>
```

where

<T1>	Disables the trunk group.
<T1> lacp	Disables LACP in the trunk group.
<T1> interface <port-list>	Removes ports from the trunk group.

- An example is shown next.
- Disable the trunk group.
- Disable LAPC on the trunk group.
- Remove ports 17 and 18 from the trunk group.

```
sysname(config)# no trunk T1
sysname(config)# no trunk T1 lacp
sysname(config)# no trunk T1 interface 17, 18
```

33.8.4 no port-access-authenticator

Syntax:

```
no port-access-authenticator
no port-access-authenticator <port-list> reauthenticate
no port-access-authenticator <port-list>
```

where

	= Disables port authentication on the switch.
<port-list> reauthenticate	= Disables the re-authentication mechanism on the listed port(s).
<port-list>	= Disables authentication on the listed ports.

An example is shown next.

- Disable authentication on the switch.
- Disable re-authentication on ports one, three, four and five.
- Disable authentication on ports one, six and seven.

```
sysname(config)# no port-access-authenticator
sysname(config)# no port-access-authenticator 1,3-5 reauthenticate
sysname(config)# no port-access-authenticator 1,6-7
```

33.8.5 no ssh

Syntax:

```
no ssh key <rsa1|rsa|dsa>
no ssh known-hosts <host-ip>
no ssh known-hosts <host-ip> [1024|ssh-rsa|ssh-dsa]
```

where

key <rsa1 rsa dsa>	Disables the secure shell server encryption key. Your switch supports SSH versions 1 and 2 using RSA and DSA authentication.
known-hosts <host-ip>	Remove specific remote hosts from the list of all known hosts.
known-hosts <host-ip> [1024 ssh-rsa ssh-dsa]	Remove remote known hosts with a specified public key (1024-bit RSA1, RSA or DSA).

An example is shown next.

- Disable the secure shell RSA1 encryption key.
- Remove the remote host with IP address 172.165.1.8 from the list of known hosts.

- Remove the remote host with IP address 172.165.1.9 and with an SSH-RSA encryption key from the list of known hosts.

```
sysname(config)# no ssh key rsa1
sysname(config)# no ssh known-hosts 172.165.1.8
sysname(config)# no ssh known-hosts 172.165.1.9 ssh-rsa
```

33.9 interface Commands

These are some commonly used commands that belong to the `interface` group of commands.

33.9.1 interface port-channel

Syntax:

```
interface port-channel <port-list>
```

Use this command to enable the specified ports for configuration. Type multiple ports or port ranges separated by a comma. Ranges of port numbers are typed separated by a dash.

The following example shows you how to access the interface command mode to configure ports 1, 3, 4 and 5.

- Enter the configuration mode.
- Enable ports one, three, four and five for configuration.
- Begin configuring for those ports.

```
sysname# config
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)#
```

33.9.2 bpd-control

Syntax:

```
bpd-control <peer|tunnel|discard|network>
```

where

<pre><peer tunnel discard network = ></pre>	<p>Type <code>peer</code> to process any BPDUs received on these ports.</p> <p>Type <code>tunnel</code> to forward BPDUs received on these ports.</p> <p>Type <code>discard</code> to drop any BPDUs received on these ports.</p> <p>Type <code>network</code> to process and forward BPDUs with a VLAN tag and to process untagged BPDUs.</p>
---	--

An example is shown next.

- Enable ports one, three, four and five for configuration.
- Set the BPDU control to `tunnel`, to forward BPDUs received on ports one, three, four and five.

```
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)# bpdu-control tunnel
sysname(config-interface)#
```

33.9.3 broadcast-limit

Syntax:

```
broadcast-limit
broadcast-limit <pkt/s>
```

where

Enables broadcast storm control limit on the switch.

<pkt/s> Sets how many broadcast packets the interface receives per second.

An example is shown next.

- Enable port one for configuration.
- Enable broadcast control.
- Set the number of broadband packets the interface receives per second.

```
sysname(config)# interface port-channel 1
sysname(config-interface)# broadcast-limit
sysname(config-interface)# broadcast-limit 21
```

33.9.4 bandwidth-limit

Syntax:

```
bandwidth-limit
bandwidth-limit egress <Kbps>
bandwidth-limit ingress <Kbps>
```

where

Enables bandwidth control on the switch.

<Kbps> Sets the maximum bandwidth allowed for outgoing traffic (egress) or incoming traffic (ingress) on the switch.

An example is shown next.

- Enable port one for configuration.
- Enable bandwidth control.
- Set the outgoing traffic bandwidth limit to 7Mbps.

- Set the incoming traffic bandwidth limit to 9Mbps.

```
sysname(config)# interface port-channel 1
sysname(config-interface)# bandwidth-limit
sysname(config-interface)# bandwidth-limit egress 7000
sysname(config-interface)# bandwidth-limit ingress 9000
```

33.9.5 mirror

Syntax:

```
mirror
mirror dir <ingress|egress|both>
```

where

Enables port mirroring on the interface.

<ingress|egress|both> = Enables port mirroring for incoming, outgoing or both incoming and outgoing traffic.

Port mirroring copies traffic from one or all ports to another or all ports for external analysis.

An example is shown next.

- Enable port mirroring.
- Enable the monitor port three.
- Enable ports one, four, five and six for configuration.
- Enable port mirroring on the ports.
- Enable port mirroring for outgoing traffic. Traffic is copied from ports one, four, five and six to port three in order to examine it in more detail without interfering with the traffic flow on the original port(s).

```
sysname(config)# mirror
sysname(config)# mirror monitor-port 3
sysname(config)# mirror mirrored-port 1
sysname(config)# mirror mirrored-port 4
sysname(config)# mirror mirrored-port 5
sysname(config)# mirror mirrored-port 6
sysname(config-interface)# mirror dir egress
```

33.9.6 gvrp

Syntax:

```
gvrp
```

GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network. Enable this function to permit VLANs groups beyond the local switch.

An example is shown next.

- Enable the IEEE 802.1Q tagged VLAN command to configure tagged VLAN for the switch.
- Enable ports one, three, four and five for configuration.
- Enable GVRP on the interface.

```
sysname(config)# vlan1q gvrp
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)# gvrp
```

33.9.7 ingress-check

Syntax:

```
ingress-check
```

Enables the device to discard incoming frames for VLANs that are not included in a port member set.

An example is shown next.

- Enable ports one, three, four and five for configuration.
- Enable ingress checking on the interface.

```
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)# ingress-check
```

33.9.8 frame-type

Syntax:

```
frame-type <all|tagged|untagged>
```

where

<pre><all tagged untagged></pre>	Choose to accept both tagged and untagged incoming frames or just tagged or untagged incoming frames on a port.
--	---

An example is shown next.

- Enable ports one, three, four and five for configuration.
- Enable ingress checking on the ports.
- Enable tagged frame-types on the interface.

```
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)# ingress-check
sysname(config-interface)# frame-type tagged
```

33.9.9 egress set

Syntax:

```
egress set <port-list>
```


where

`<port-list>` Sets the outgoing traffic port list for a port-based VLAN.

An example is shown next.

- Enable port-based VLAN tagging on the switch.
- Enable ports one, three, four and five for configuration.
- Set the outgoing traffic ports as the CPU (0), seven (7), eight (8) and nine (9).

```
sysname(config)# vlan-type port-based
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)# egress set 0,7-9
```

33.9.10 qos priority

Syntax:

`qos priority <0 .. 7>`

where

`<0 .. 7>` Sets the quality of service priority for a port.

An example is shown next.

- Enable ports one, three, four and five for configuration.
- Set the IEEE 802.1p quality of service priority as four (4).

```
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)# qos priority 4
```

33.9.11 name

Syntax:

`name <port-name-string>`

where

`<port-name-string>` Sets a name for your port interface(s).

An example is shown next.

- Enable ports one, three, four and five for configuration.
- Set a name for the ports.

```
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)# name Test
```

33.9.12 speed-duplex

Syntax:

```
speed-duplex <auto|10-half|10-full|100-half|100-full|1000-full>
```

where

<pre><auto 10-half 10- full 100-half 100- full 1000-full></pre>	Sets the duplex mode (half or full) and speed (10, 100 or 1000 Mbps) of the connection on the port. Selecting auto (auto-negotiation) makes one port able to negotiate with a peer automatically to obtain the connection speed and duplex mode that both ends support.
---	---

An example is shown next.

- Enable ports one, three, four and five for configuration.
- Set the speed to 10 Mbps in half duplex mode.

```
sysname(config)# interface port-channel 1,3-5  
sysname(config-interface)# speed-duplex 10-half
```

IEEE 802.1Q Tagged VLAN Commands

This chapter describes the IEEE 802.1Q Tagged VLAN and associated commands.

34.1 Configuring Tagged VLAN

Refer to [Chapter 7 on page 87](#) for background information on VLANs.

The following procedure shows you how to configure tagged VLAN.

- 1 Use the IEEE 802.1Q tagged VLAN commands to configure tagged VLAN for the switch.
 - Use the `vlan <vlan-id>` command to configure or create a VLAN on the switch. The switch automatically enters the `config-vlan` mode. Use the `inactive` command to deactivate the VLAN(s).
 - Use the `interface port-channel <port-list>` command to enter the `config-interface` mode to set the VLAN settings on a port, then use the `pvid <vlan-id>` command to set the VLAN ID you created for the port-list to that specific port in the PVID table.
 - Use the `exit` command when you are finished configuring the VLAN.

Example:

```
sysname(config)# vlan 2000
sysname(config-vlan)# name up1
sysname(config-vlan)# fixed 10-12
sysname(config-vlan)# no untagged 10-12
sysname(config-vlan)# exit
sysname(config)# interface port-channel 10-12
sysname(config-interface)# pvid 2000
sysname(config-interface)# exit
```

- 2 Configure your management VLAN.
 - Use the `vlan <vlan-id>` command to create a VLAN (VID 3 in this example) for managing the switch, and the switch will activate the new management VLAN.
 - Use the `inactive` command to disable the new management VLAN.

Example:

```
sysname(config)# vlan 3
sysname(config-vlan)# inactive
```

34.2 Global VLAN1Q Tagged VLAN Configuration Commands

This section shows you how to configure and monitor the IEEE 802.1Q Tagged VLAN.

34.2.1 GARP Status

Syntax:

```
show garp
```

This command shows the switch's GARP timer settings, including the join, leave and leave all timers.

An example is shown next.

```
sysname# show garp
GARP Timer
-----
Join Timer = 200
Leave Timer = 600
Leave All Timer = 10000
sysname#
```

34.2.2 GARP Timer

Syntax:

```
garp join <msec> leave <msec> leaveall <msec>
```

where

- | | | |
|--------------------|---|---|
| join <msec> | = | This sets the duration of the Join Period timer for GVRP in milliseconds. Each port has a Join Period timer. The allowed Join Time range is between 100 and 32767 milliseconds; the default is 200 milliseconds. |
| leave <msec> | = | This sets the duration of the Leave Period timer for GVRP in milliseconds. Each port has a single Leave Period timer. Leave Time must be two times larger than Join Timer; the default is 600 milliseconds. |
| leaveall
<msec> | = | This sets the duration of the Leave All Period timer for GVRP in milliseconds. Each port has a single Leave All Period timer. Leave All Timer must be larger than Leave Timer; the default is 10000 milliseconds. |

This command sets the switch's GARP timer settings, including the join, leave and leave all timers.

Switches join VLANs by making a declaration. A declaration is made by issuing a Join message using GARP. Declarations are withdrawn by issuing a Leave message. A Leave All message terminates all registrations. GARP timers set declaration timeout values.

The following example sets the Join Timer to 300 milliseconds, the Leave Timer to 800 milliseconds and the Leave All Timer to 11000 milliseconds.

```
sysname(config)# garp join 300 leave 800 leaveall 11000
```

34.2.3 GVRP Timer

Syntax:

```
show vlan1q gvrp
```

This command shows the switch's GVRP settings.

An example is shown next.

```
sysname# show vlan1q gvrp
GVRP Support
-----
gvrpEnable = YES
GVRP Support
```

34.2.4 Enable GVRP

Syntax:

```
vlan1q gvrp
```

This command turns on GVRP in order to propagate VLAN information beyond the switch.

34.2.5 Disable GVRP

Syntax:

```
no vlan1q gvrp
```

This command turns off GVRP so that the switch does not propagate VLAN information to other switches.

34.3 Port VLAN Commands

You must configure the switch port VLAN settings in config-interface mode.

34.3.1 Set Port VID

Syntax:

```
pvid <VID>
```

where

<VID> = Specifies the VLAN number between 1 and 4094

This command sets the default VLAN ID on the port(s).

The following example sets the default VID to 200 on ports 1 to 5.

```
sysname(config)# interface port-channel 1-5
sysname(config-interface)# pvid 200
```

34.3.2 Set Acceptable Frame Type

Syntax:

```
frame-type <all|tagged>
```

where

<all|tagged> = Specifies all Ethernet frames (tagged and untagged) or only tagged Ethernet frames.

This command sets the specified port to accept all Ethernet frames or only those with an IEEE 802.1Q VLAN tag.

The following example sets ports 1 to 5 to accept only tagged frames.

```
sysname(config)# interface port-channel 1-5
sysname(config-interface)# frame-type tagged
```

34.3.3 Enable or Disable Port GVRP

Use the `gvrp` command to enable GVRP on the port(s). Use the `no gvrp` command to disable GVRP.

The following example turns off GVRP for ports 1 to 5.

```
sysname(config)# interface port-channel 1-5
sysname(config-interface)# no gvrp
```

34.3.4 Modify Static VLAN

Use the following commands in the `config-vlan` mode to configure the static VLAN table.

Syntax:

```

vlan <vlan-id>
fixed <port-list>
forbidden <port-list>
name <name-str>
normal <port-list>
untagged <port-list>
no fixed <port-list>
no forbidden <port-list>
no untagged <port-list>

```

where

<vlan-id> = The VLAN ID [1 – 4094].
 <name-str> = A name to identify the SVLAN entry.
 <port-list> = This is the switch port list.

- Enter `fixed` to register the <port-list> to the static VLAN table with <vlan-id>.
- Enter `normal` to confirm registration of the <port-list> to the static VLAN table with <vlan-id>.
- Enter `forbidden` to block a <port-list> from joining the static VLAN table with <vlan-id>.
- Enter `no fixed` or `no forbidden` to change <port-list> to normal status.
- Enter `untagged` to send outgoing frames without a tag.
- Enter `no untagged` to tag outgoing frames.

The following example configures ports 1 to 5 as fixed and untagged ports in VLAN 2000.

```

sysname(config)# vlan 2000
sysname(config-vlan)# fixed 1-5
sysname(config-vlan)# untagged 1-5

```

34.3.5 Forwarding Process Example

34.3.5.1 Tagged Frames

- 1 First the switch checks the VLAN ID (VID) of tagged frames or assigns temporary VIDs to untagged frames.
- 2 The switch then checks the VID in a frame's tag against the SVLAN table.
- 3 The switch notes what the SVLAN table says (that is, the SVLAN tells the switch whether or not to forward a frame and if the forwarded frames should have tags).
- 4 Then the switch applies the port filter to finish the forwarding decision. This means that frames may be dropped even if the SVLAN says to forward them. Frames might also be dropped if they are sent to a CPE (customer premises equipment) DSL device that does not accept tagged frames.

34.3.5.2 Untagged Frames

- 1 An untagged frame comes in from the LAN.
- 2 The switch checks the PVID table and assigns a temporary VID of 1.

- 3 The switch ignores the port from which the frame came, because the switch does not send a frame to the port from which it came. The switch also does not forward frames to “forbidden” ports.
- 4 If after looking at the SVLAN, the switch does not have any ports to which it will send the frame, it won’t check the port filter.

34.4 Delete VLAN ID

Syntax:

```
no vlan <vlan-id>
```

where

<vlan-id> = The VLAN ID [1 – 4094].

This command deletes the specified VLAN ID entry from the static VLAN table. The following example deletes entry 2 in the static VLAN table.

```
sysname(config)# no vlan 2
```

34.5 Enable VLAN

Syntax:

```
vlan <vlan-id>
```

This command enables the specified VLAN ID in the SVLAN (Static VLAN) table.

34.6 Disable VLAN

Syntax:

```
vlan <vlan-id>  
inactive
```

This command disables the specified VLAN ID in the SVLAN (Static VLAN) table.

34.7 Show VLAN Setting

Syntax:

```
show vlan
```

This command shows the IEEE 802.1Q Tagged SVLAN (Static VLAN) table.

An example is shown next.

```
sysname# show vlan
The Number of VLAN :      2
Idx.  VID    Status      Elap-Time    TagCtl
----  -
      1      1      Static      0:54:40    Untagged :1-18
                                   Tagged   :
      2      2      Static      0:54:41    Untagged :
                                   Tagged   :
sysname#
```


Troubleshooting

This chapter covers potential problems and possible remedies.

35.1 Problems Starting Up the Switch

Table 87 Troubleshooting the Start-Up of Your Switch

PROBLEM	CORRECTIVE ACTION
None of the LEDs turn on when you turn on the switch.	Check the power connection and make sure the power source is turned on.
	If the error persists, you may have a hardware problem. In this case, you should contact your vendor.

35.2 Problems Accessing the Switch

Table 88 Troubleshooting Accessing the Switch

PROBLEM	CORRECTIVE ACTION
I cannot access the switch using Telnet.	<p>Make sure the ports are properly connected.</p> <p>You may have exceeded the maximum number of concurrent Telnet sessions. Close other Telnet session(s) or try connecting again later.</p> <p>Check that you have enabled Telnet service access. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on access control for details.</p>
I cannot access the web configurator.	<p>The administrator username is "admin". The default administrator password is "1234". The username and password are case-sensitive. Make sure that you enter the correct password and username using the proper casing. If you have changed the password and have now forgotten it, you will need to upload the default configuration file. This restores all of the factory defaults including the password.</p> <p>If you have configured more than one IP interface, make sure another administrator is NOT logged into the web configurator on a different IP interface using the same account.</p> <p>Check that you have enabled web service access. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on access control for details.</p> <p>Your computer's and the switch's IP addresses must be on the same subnet.</p> <p>See the following section to check that pop-up windows, JavaScripts and Java permissions are allowed.</p>

35.3 Problem with the VDSL Connection

Table 89 Troubleshooting VDSL Connection

PROBLEM	CORRECTIVE ACTION
The VDSL link is down.	<p>Make sure the VDSL port is activated.</p> <p>Check the port connection. Make sure the cable is faulty.</p> <p>The VDSL port may be faulty. Try connecting to a different VDSL port on the switch.</p> <p>The target transmission rate(s) may be too high. Set the switch to use a lower link transmission rate.</p> <p>The CPE device may be faulty. Try connecting another CPE device to the VDSL port.</p>
Cannot send traffic over the VDSL link.	<p>Make sure the VDSL port is activated and that the physical link status is up.</p> <p>Check that the traffic on this VDSL port is not blocked by the filter settings on the switch.</p> <p>Check the MAC address learning limitation on the VDSL port. Make sure the maximum number of MAC address is not reached or turn off this feature.</p> <p>Make sure the VDSL client IP address is configured correctly.</p> <p>Check the VLAN settings on the switch. Make sure the VLAN group, VLAN ID and egress settings are correct on the VDSL port.</p>

35.3.1 Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).



Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

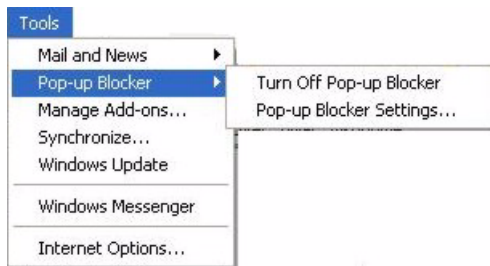
35.3.1.1 Internet Explorer Pop-up Blockers

You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

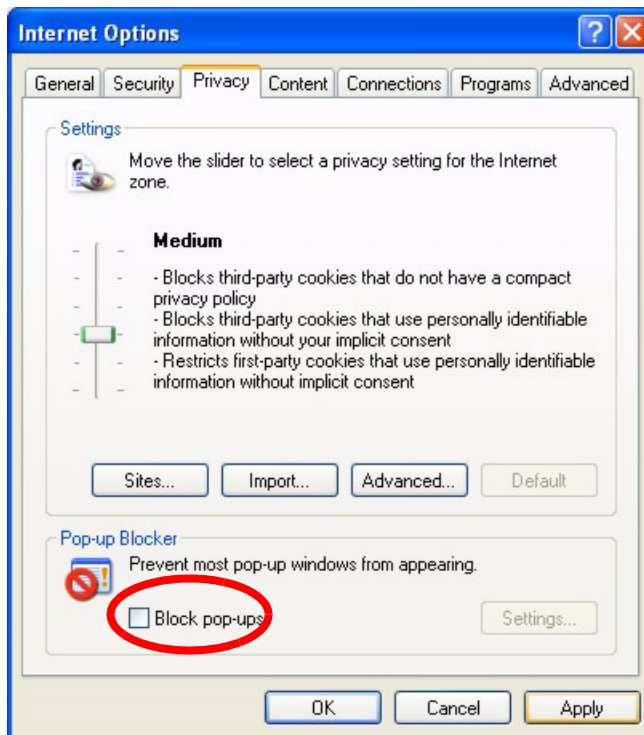
35.3.1.1.1 Disable pop-up Blockers

- 1 In Internet Explorer, select **Tools, Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 108 Pop-up Blocker

You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

- 1 In Internet Explorer, select **Tools, Internet Options, Privacy**.
- 2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

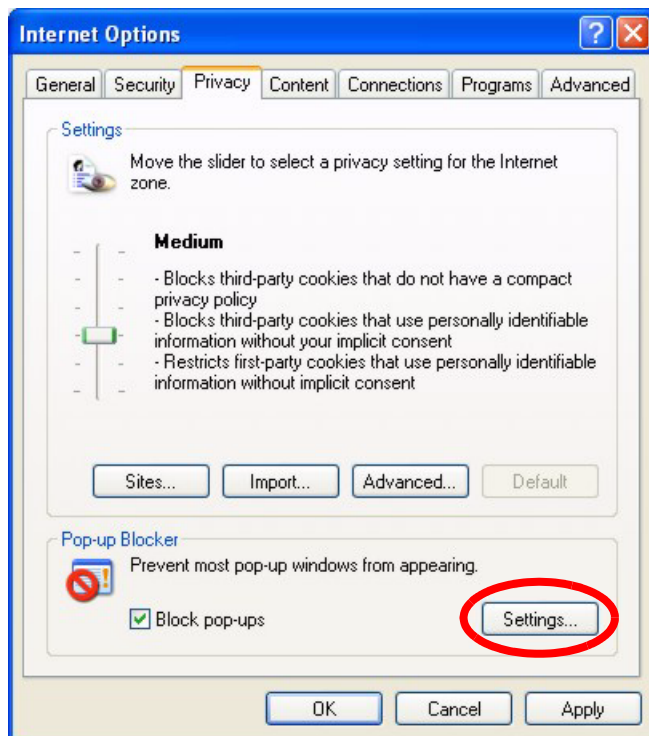
Figure 109 Internet Options

- 3 Click **Apply** to save this setting.

35.3.1.1.2 Enable pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

- 1 In Internet Explorer, select **Tools, Internet Options** and then the **Privacy** tab.
- 2 Select **Settings...** to open the **Pop-up Blocker Settings** screen.

Figure 110 Internet Options

- 3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.1.1.
- 4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 111 Pop-up Blocker Settings

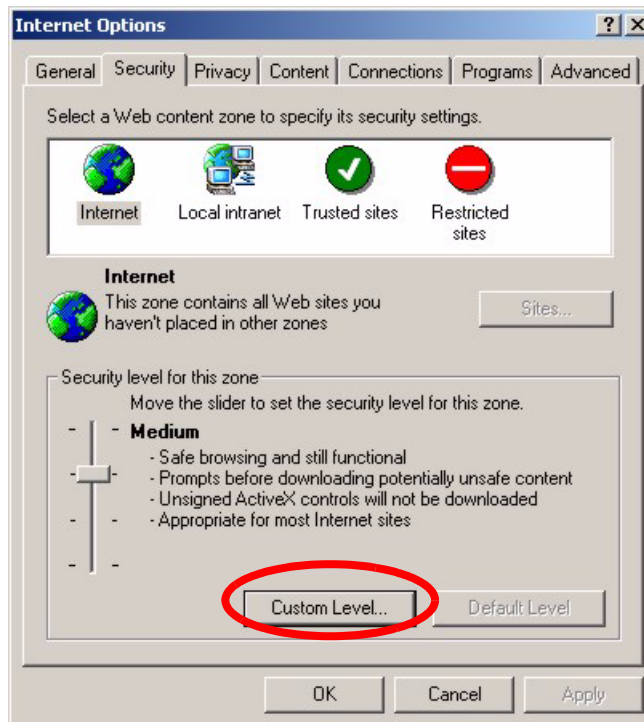
- 5 Click **Close** to return to the **Privacy** screen.
- 6 Click **Apply** to save this setting.

35.3.1.2 JavaScripts

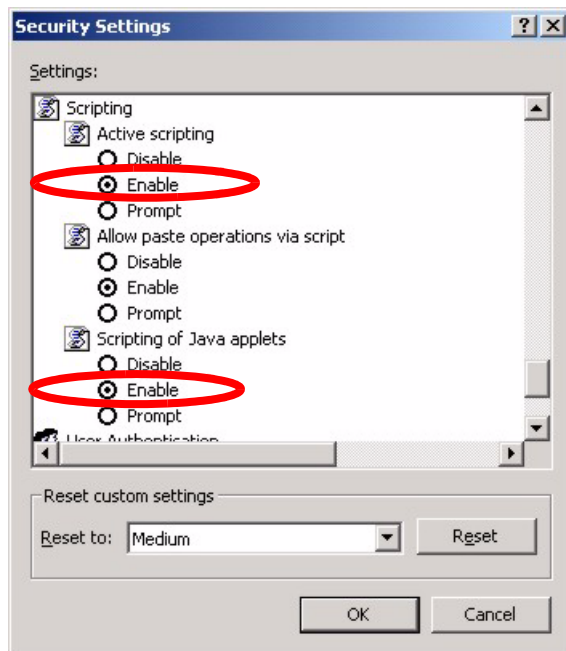
If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

- 1 In Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.

Figure 112 Internet Options

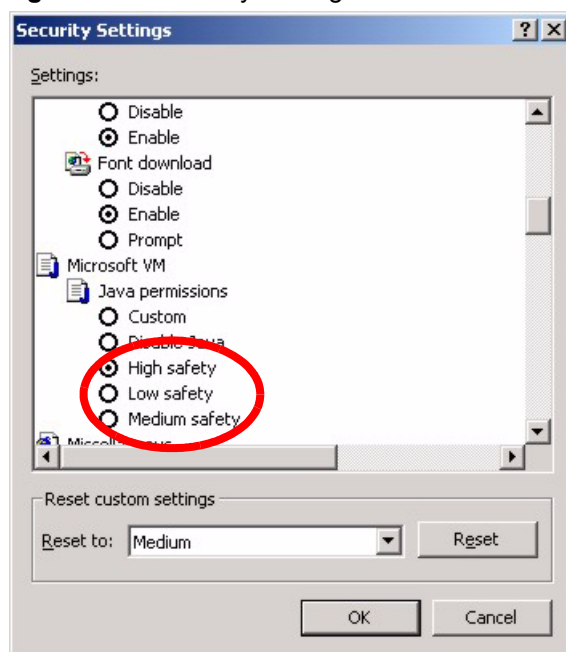


- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Scripting**.
- 4 Under **Active scripting** make sure that **Enable** is selected (the default).
- 5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).
- 6 Click **OK** to close the window.

Figure 113 Security Settings - Java Scripting

35.3.1.3 Java Permissions

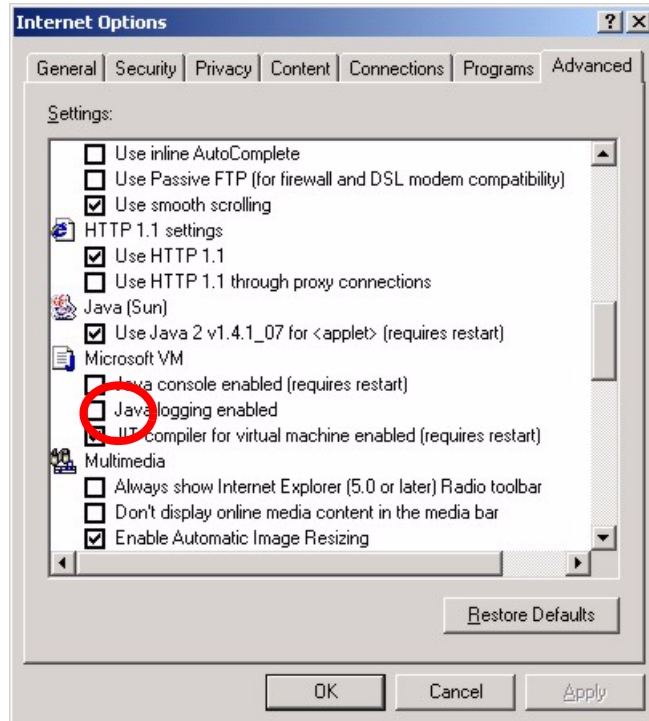
- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.
- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Microsoft VM**.
- 4 Under **Java permissions** make sure that a safety level is selected.
- 5 Click **OK** to close the window.

Figure 114 Security Settings - Java

35.3.1.3.1 JAVA (Sun)

- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Advanced** tab.
- 2 make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.
- 3 Click **OK** to close the window.

Figure 115 Java (Sun)



35.4 Problems with the Password

Table 90 Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
Cannot access the switch.	<p>The password field is case sensitive. Make sure that you enter the correct password using the proper casing.</p> <p>The administrator username is "admin". The default administrator password is "1234". The username and password are case-sensitive. Make sure that you enter the correct password and username using the proper casing.</p> <p>If you have changed the password and have now forgotten it, you will need to upload the default configuration file. This restores all of the factory defaults including the password.</p>

Product Specifications

These are the switch product specifications.

Table 91 Product Specifications

General Product Specifications	
Standards	IEEE802.3 10BASE-T Ethernet (twisted-pair copper) IEEE802.3u 100BASE-TX Fast Ethernet (twisted-pair copper) ANSI/IEEE802.3 Auto-negotiation IEEE802.3x Flow Control IEEE802.1p Priority Queues IEEE802.1Q Tagged VLAN
VDSL	One Telco connector for 16 VDSL or POTS/ISDN lines Duplex Method: DMT/FDD Band Plan: 998 Tone spacing: 4.3125 - 8.625 KHz +/- 50 ppm Upstream speed: 100 Mbps or 50 Mbps (VDSL1) or 30 Mbps (VDSL2) Downstream speed: 100 Mbps (VDSL1) or 50 Mbps (VDSL2) Optional band: 25 ~ 138 K (VES-1616F-34), 138 ~ 276 K (VES-1616F-35)
Interfaces	Two Gigabit/mini-GBIC uplink ports One Console port (DB-9 female) Telco 50 (for VDSL and POTS/ISDN lines)
Performance and Management Specifications	
VDSL	Fixed Rate and Rate Adaptive. Power back off Interleave delay setting RFI configuration Resynchronization
Diagnostics Capabilities	The switch can perform self-diagnostic tests. These tests check the operation of the following circuits: FLASH memory DRAM LAN port local and remote loopback test Per VDSL port loopback test HTP items
VLAN	IEEE 802.1Q tag-based VLAN, 4094 Max Port-based VLAN Up to 256 VLAN groups Multicast VLAN Registration (MVR): 3 groups

Table 91 Product Specifications (continued)

Security	Static MAC address forward MAC address learning: 10 per port Block unresolved address forwarding/Port security 802.1x port authentication
Multicasting	Support IGMP snooping and filtering IGMP V1 and V2 (RFC2236 and RFC112)
Bridging	16K MAC addresses learning Static MAC address forwarding, 256 entries Broadcast storm control Automatic address learning and aging Aging time from 10 to 765 seconds in 1 second increment (default 300 seconds) Transparent bridging
Switching	6.4 Gbps, non-blocking Maximum frame size: 1522 bytes including tag/CRC Store and forward
QoS	IEEE 802.1p Eight priority queues Queuing Algorithm: SP/WFS Port-based bandwidth control from 100Kbps to 100Mbps (by 1518bytes packets) DiffServ (RFC 2475)
STP	IEEE 802.1d IEEE 802.1w
Port Mirroring	Port based mirroring to a monitor port
Broadcast Storm	Support broadcast storm control
Port Aggregation	One aggregation group LACP support
DHCP	DHCP server/relay DHCP relay Option82
System Management	Configuration via console/telnet/web Firmware upgrade via FTP/web/console Configuration backup and restore via FTP/web/console System management access control Multi-login, single management. System clock: manual setup or NTP SNMP v2c RMON group 1,2,3,9 ICMP echo/echo reply
CPE Device Management	Remote CPE firmware upgrade via the web configurator Remote CPE line reset/retrain
Management Security	User ID/Password for Telnet and Web-based management authentication Up to five login accounts.

Table 91 Product Specifications (continued)

MIBs	RFC1213 RFC1493 Bridge MIB RFC1643 Ethernet MIB RFC1757 RMON RFC1155 SMI RFC 2233 ifVHCPacketGroup RFC 2647 Bridge MIB extension (for 802.1Q) RFC 2925 PING-MIB and TRACEROUTE-MIB RFC 3728 VDSL line MIB
Physical and Environmental Specifications	
Weight	< 8kg
Power Supply	100 - 240 V, 50/60 Hz AC
Power Consumption	75 W (max.)
Temperature Threshold	Three temperature sensors: T1 (VDSL Chipset): 81 °C ON; 60 °C OFF T2 (Switch): 73 °C ON; 65 °C OFF T3 (Monitor chipset): 88 °C ON; 60 °C OFF
Voltage Threshold	Four voltages: 2.5V: +- 6% 1.2V: +- 6% 3.5V: +- 6% 12V: +- 6%
Operating Temperature	0 ~ 50°C
Storage Temperature	-25 ~ 70°C
Operational Humidity	10 ~ 90% (non-condensing)
Safety	UL60950-1 CSA60950-1 EN60950 -1 IEC60950-1 ITU-T K.20 (Version 2000)
EMC	CE-EMC Class A FCC Part 15 Class A

The following table lists the splitter board specifications.

Table 92 CO Impedance Splitter Board Specifications

COUNTRY	POTS	ISDN
Belgium	270Ω+ (750Ω//150nF)	135Ω (2B1Q)
Taiwan	900Ω	None (POTS only)
Denmark	270Ω+ (750Ω//150nF)	None (POTS only)
Finland	270Ω+ (750Ω//150nF)	None (POTS only)
France	270Ω+ (750Ω//150nF)	135Ω (2B1Q)
Germany	220Ω + (820Ω//115nF)	150Ω (4B3T)
Iceland	270Ω+ (750Ω//150nF)	None (POTS only)

Table 92 CO Impedance Splitter Board Specifications (continued)

COUNTRY	POTS	ISDN
Netherlands	270Ω+ (750Ω//150nF)	135Ω (2B1Q)
Norway	270Ω+ (750Ω//150nF)	135Ω (2B1Q)
Russia	600Ω	None (POTS only)
Sweden	270Ω+ (750Ω//150nF)	None (POTS only)
Swiss	270Ω+ (750Ω//150nF)	135Ω (2B1Q)
UK	320Ω + (1050Ω//230nF)	None (POTS only)
USA	900Ω	None (POTS only)

Hardware Telco-50 Connector Pin Assignments

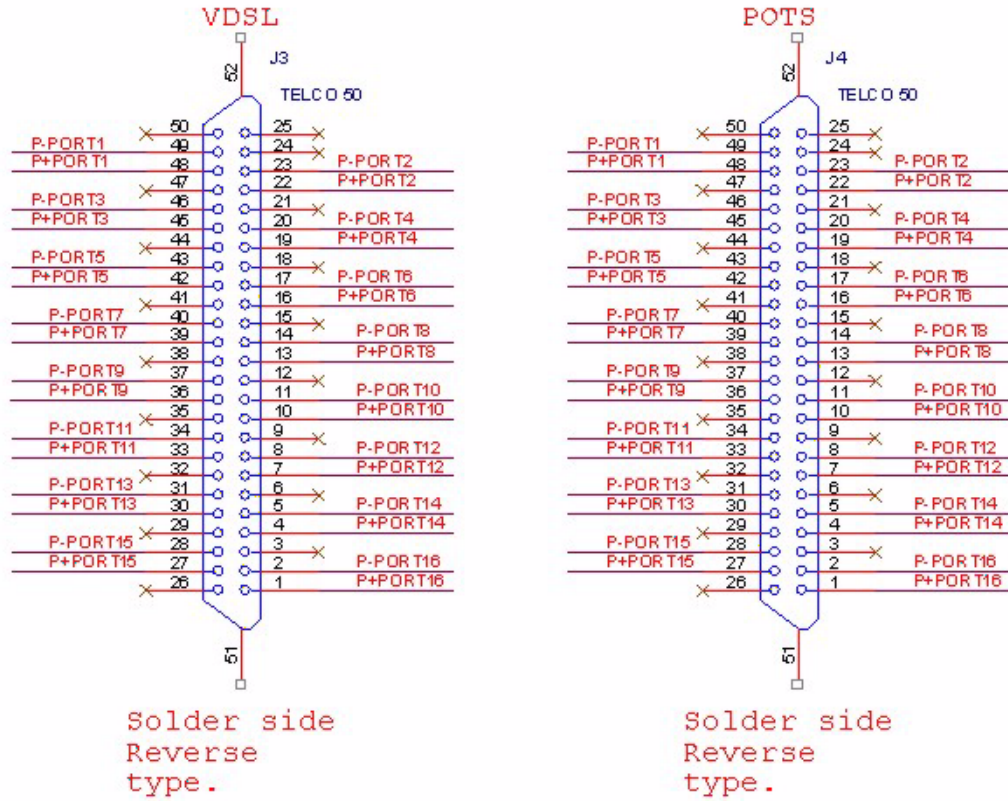
The following table and diagram show the pin assignments of the Telco-50 connectors on the switch.

Table 93 Hardware Telco-50 Pin Assignments

VDSL				POTS/ISDN			
PIN1	P+PORT16	PIN26	NULL	PIN1	P+PORT16	PIN26	NULL
PIN2	P-PORT16	PIN27	P+PORT15	PIN2	P-PORT16	PIN27	P+PORT15
PIN3	NULL	PIN28	P-PORT15	PIN3	NULL	PIN28	P-PORT15
PIN4	P+PORT14	PIN29	NULL	PIN4	P+PORT14	PIN29	NULL
PIN5	P-PORT14	PIN30	P+PORT13	PIN5	P-PORT14	PIN30	P+PORT13
PIN6	NULL	PIN31	P-PORT13	PIN6	NULL	PIN31	P-PORT13
PIN7	P+PORT12	PIN32	NULL	PIN7	P+PORT12	PIN32	NULL
PIN8	P-PORT12	PIN33	P+PORT11	PIN8	P-PORT12	PIN33	P+PORT11
PIN9	NULL	PIN34	P-PORT11	PIN9	NULL	PIN34	P-PORT11
PIN10	P+PORT10	PIN35	NULL	PIN10	P+PORT10	PIN35	NULL
PIN11	P-PORT10	PIN36	P+PORT9	PIN11	P-PORT10	PIN36	P+PORT9
PIN12	NULL	PIN37	P-PORT9	PIN12	NULL	PIN37	P-PORT9
PIN13	P+PORT8	PIN38	NULL	PIN13	P+PORT8	PIN38	NULL
PIN14	P-PORT8	PIN39	P+PORT7	PIN14	P-PORT8	PIN39	P+PORT7
PIN15	NULL	PIN40	P-PORT7	PIN15	NULL	PIN40	P-PORT7
PIN16	P+PORT6	PIN41	NULL	PIN16	P+PORT6	PIN41	NULL
PIN17	P-PORT6	PIN42	P+PORT5	PIN17	P-PORT6	PIN42	P+PORT5
PIN18	NULL	PIN43	P-PORT5	PIN18	NULL	PIN43	P-PORT5
PIN19	P+PORT4	PIN44	NULL	PIN19	P+PORT4	PIN44	NULL
PIN20	P-PORT4	PIN45	P+PORT3	PIN20	P-PORT4	PIN45	P+PORT3
PIN21	NULL	PIN46	P-PORT3	PIN21	NULL	PIN46	P-PORT3
PIN22	P+PORT2	PIN47	NULL	PIN22	P+PORT2	PIN47	NULL
PIN23	P-PORT2	PIN48	P+PORT1	PIN23	P-PORT2	PIN48	P+PORT1

Table 93 Hardware Telco-50 Pin Assignments

PIN24	NULL	PIN49	P-POR T1	PIN24	NULL	PIN49	P-POR T1
PIN25	NULL	PIN50	NULL	PIN25	NULL	PIN50	NULL

Figure 116 Hardware Telco-50 Pin Assignments

This table lists the ports and matching pin numbers for the hardware Telco-50 connector.

Table 94 Hardware Telco-50 Connector Port and Pin Numbers

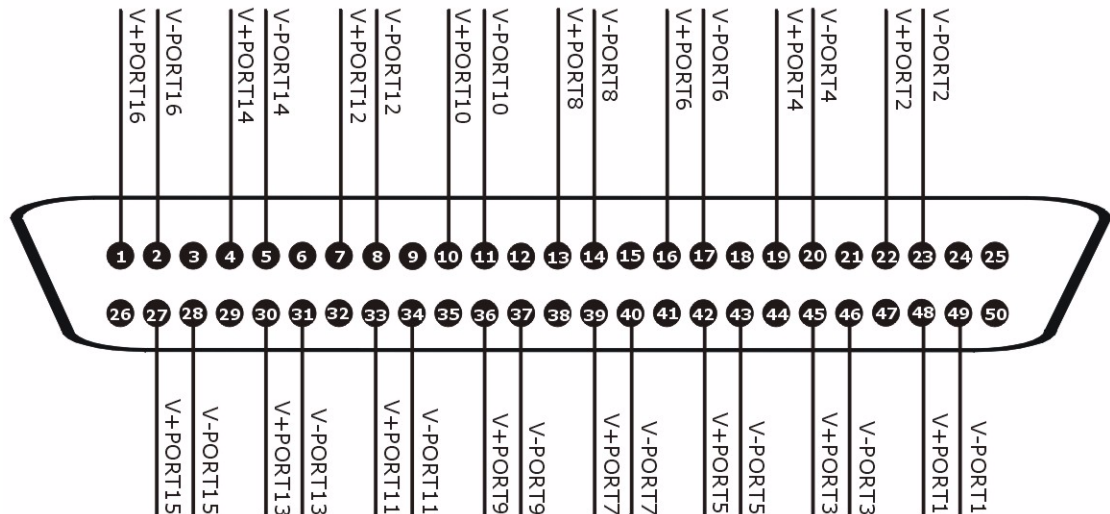
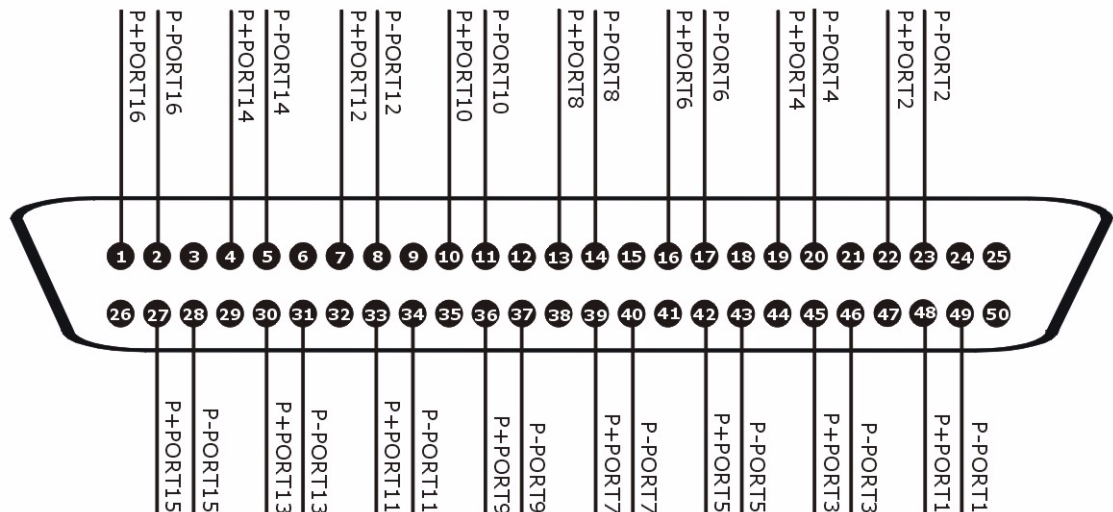
VDSL PORT NUMBER	PIN NUMBER
1	48, 49
2	22, 23
3	45, 46
4	19, 20
5	42, 43
6	16, 17
7	39, 40
8	13, 14
9	36, 37
10	10, 11
11	33, 34
12	7, 8
13	30, 31

Table 94 Hardware Telco-50 Connector Port and Pin Numbers (continued)

VDSL PORT NUMBER	PIN NUMBER
14	4, 5
15	27, 28
16	1, 2

Telco-50 Cable Telco-50 Connector Pin Assignments

Use Telco-50 cables to connect the **VDSL LINE** port to the user equipment (VDSL modem) and the **POTS/ISDN LINE** port to the central office switch or PBX (Private Branch Exchange). The following diagram shows the pin assignments that you need to have on the Telco-50 connectors on the Telco-50 cables.

Figure 117 Telco-50 Cable VDSL Telco-50 Pin Assignments**Figure 118** Telco-50 Cable POTS/ISDN Telco-50 Pin Assignments

Console Cable Pin Assignments

In a serial communications connection, generally a computer is DTE (Data Terminal Equipment) and a modem is DCE (Data Circuit-terminating Equipment). The Switch is DCE when you connect a computer to the console port. The following diagrams and chart show the pin assignments of the console cable.

The pin layout for the DB-9 connector end of the cables is as follows.

Figure 119 Console Cable DB-9 End Pin Layout

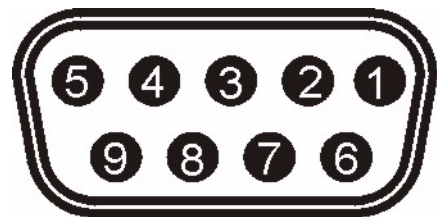


Table 95 Console Port Pin Assignments

CONSOLE Port RS – 232 (Female) DB-9F	DIAL BACKUP RS – 232 (Male) DB-9M
Pin 1 = NON	Pin 1 = NON
Pin 2 = DCE-TXD	Pin 2 = DTE-RXD
Pin 3 = DCE –RXD	Pin 3 = DTE-TXD
Pin 4 = DCE –DSR	Pin 4 = DTE-DTR
Pin 5 = GND	Pin 5 = GND
Pin 6 = DCE –DTR	Pin 6 = DTE-DSR
Pin 7 = DCE –CTS	Pin 7 = DTE-RTS
Pin 8 = DCE –RTS	Pin 8 = DTE-CTS
PIN 9 = NON	PIN 9 = NON.

PART VIII

Appendices and Index



The appendices provide general information. Some details may not apply to your Switch.

[Legal Information \(295\)](#)

[Customer Support \(299\)](#)

[Index \(303\)](#)

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

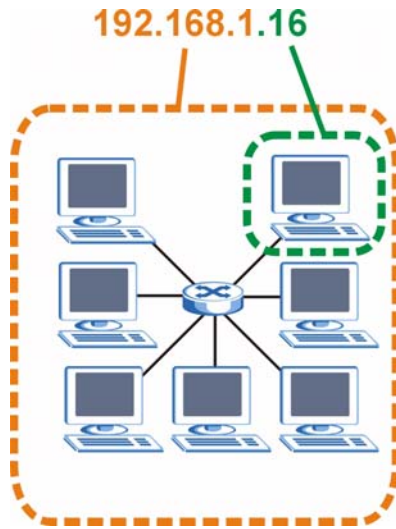
One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 120 Network Number and Host ID

How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term “subnet” is short for “sub-network”.

A subnet mask has 32 bits. If a bit in the subnet mask is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 96 IP Address Network Number and Host ID Example

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	11111111	11111111	11111111	00000000
Network Number	11000000	10101000	00000001	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a “1” value). For example, an “8-bit mask” means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 97 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 98 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} - 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} - 2$	65534
24 bits	255.255.255.0	8 bits	$2^8 - 2$	254
29 bits	255.255.255.248	3 bits	$2^3 - 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a “/” followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 99 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128

Table 99 Alternative Subnet Mask Notation (continued)

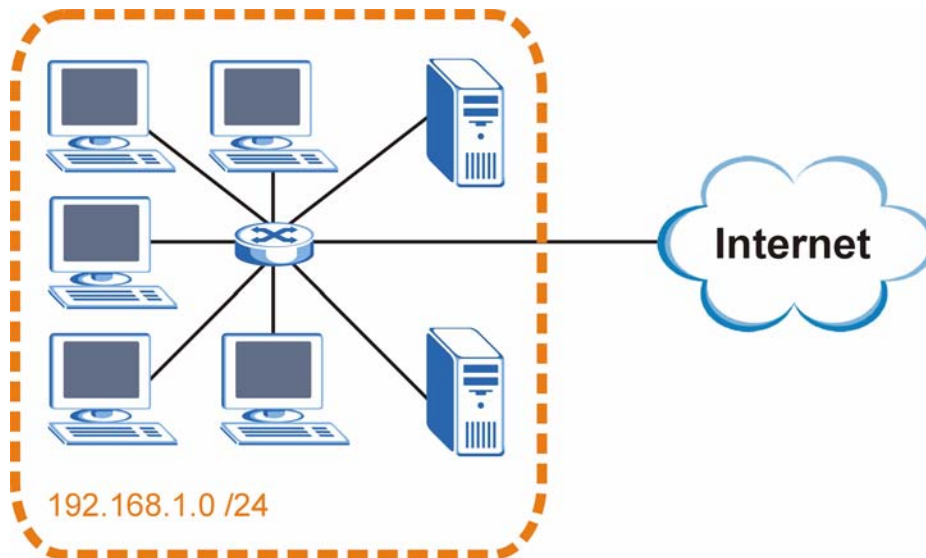
SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of $2^8 - 2$ or 254 possible hosts.

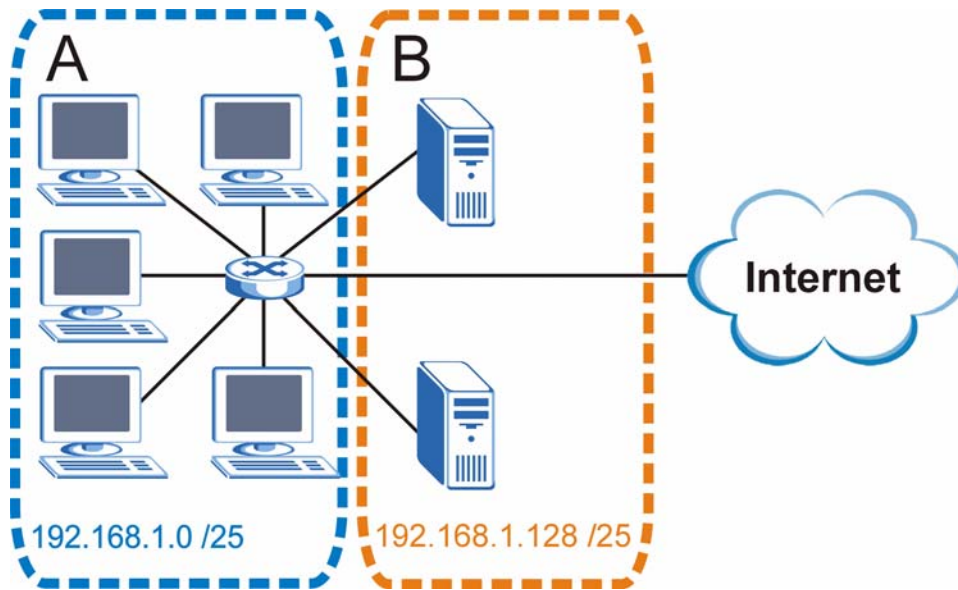
The following figure shows the company network before subnetting.

Figure 121 Subnetting Example: Before Subnetting

You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 122 Subnetting Example: After Subnetting

In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of $2^7 - 2$ or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to “borrow” two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.11000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving $2^6 - 2$ or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 100 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 101 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	01000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 102 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 103 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	11000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 104 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127

Table 104 Eight Subnets (continued)

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 105 24-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 106 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6

Table 106 16-bit Network Number Subnet Planning (continued)

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the Switch.

Once you have decided on the network number, pick an IP address for your Switch that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your Switch will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the Switch unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

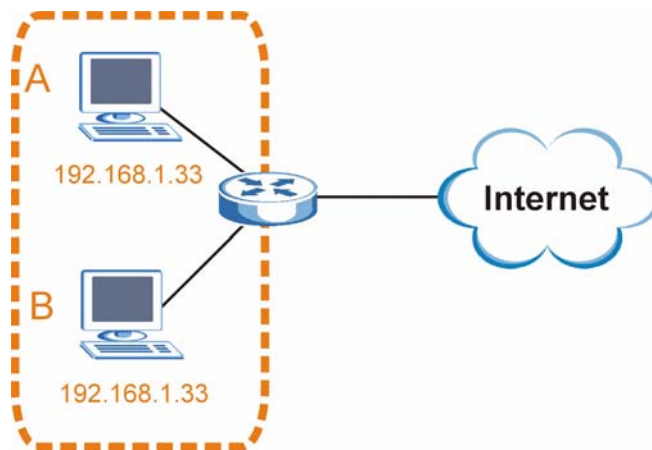
IP Address Conflicts

Each device on a network must have a unique IP address. Devices with duplicate IP addresses on the same network will not be able to access the Internet or other resources. The devices may also be unreachable through the network.

Conflicting Computer IP Addresses Example

More than one device can not use the same IP address. In the following example computer **A** has a static (or fixed) IP address that is the same as the IP address that a DHCP server assigns to computer **B** which is a DHCP client. Neither can access the Internet. This problem can be solved by assigning a different static IP address to computer **A** or setting computer **A** to obtain an IP address automatically.

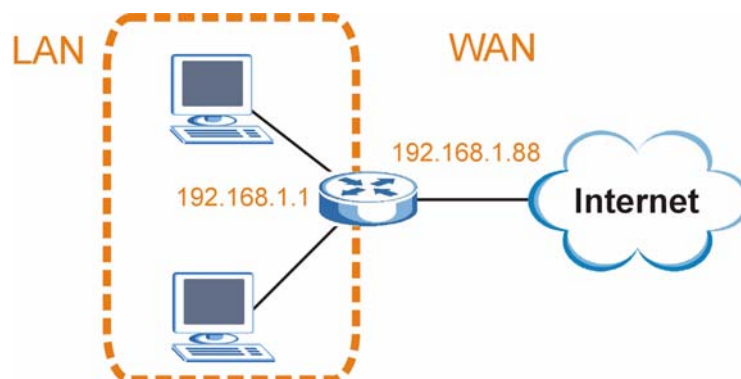
Figure 123 Conflicting Computer IP Addresses Example



Conflicting Router IP Addresses Example

Since a router connects different networks, it must have interfaces using different network numbers. For example, if a router is set between a LAN and the Internet (WAN), the router's LAN and WAN addresses must be on different subnets. In the following example, the LAN and WAN are on the same subnet. The LAN computers cannot access the Internet because the router cannot route between networks.

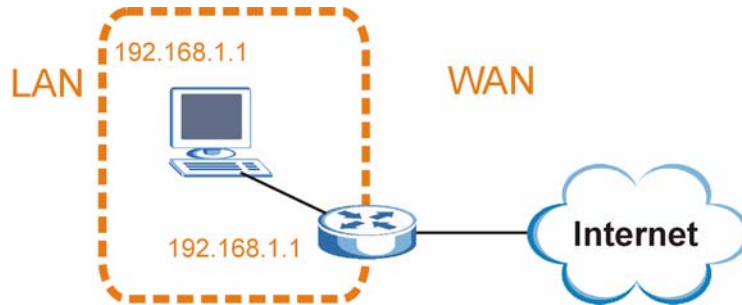
Figure 124 Conflicting Computer IP Addresses Example



Conflicting Computer and Router IP Addresses Example

More than one device can not use the same IP address. In the following example, the computer and the router's LAN port both use 192.168.1.1 as the IP address. The computer cannot access the Internet. This problem can be solved by assigning a different IP address to the computer or the router's LAN port.

Figure 125 Conflicting Computer and Router IP Addresses Example



Legal Information

Copyright

Copyright © 2007 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

FCC Warning

This device has been tested and found to comply with the limits for a Class A digital switch, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This device generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this device in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning:

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Taiwanese BSMI (Bureau of Standards, Metrology and Inspection) A Warning:

警告使用者
這是甲類的資訊產品，在居住的環境使用時，
可能造成射頻干擾，在這種情況下，
使用者會被要求採取某些適當的對策。

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

CLASS 1 LASER PRODUCT

APPAREIL A LASER DE CLASS 1

PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11.

PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11.

Viewing Certifications

- 1 Go to <http://www.zyxel.com>.
- 2 Select your product on the ZyXEL home page to go to that product's page.
- 3 Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating

condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Customer Support

Please have the following information ready when you contact customer support.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Corporate Headquarters (Worldwide)

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-3-578-3942
- Fax: +886-3-578-2439
- Web Site: www.zyxel.com, www.europe.zyxel.com
- FTP Site: [ftp.zyxel.com](ftp://ftp.zyxel.com), [ftp.europe.zyxel.com](ftp://ftp.europe.zyxel.com)
- Regular Mail: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

Costa Rica

- Support E-mail: soporte@zyxel.co.cr
- Sales E-mail: sales@zyxel.co.cr
- Telephone: +506-2017878
- Fax: +506-2015098
- Web Site: www.zyxel.co.cr
- FTP Site: [ftp.zyxel.co.cr](ftp://ftp.zyxel.co.cr)
- Regular Mail: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

Czech Republic

- E-mail: info@cz.zyxel.com
- Telephone: +420-241-091-350
- Fax: +420-241-091-359
- Web Site: www.zyxel.cz
- Regular Mail: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Česká Republika

Denmark

- Support E-mail: support@zyxel.dk
- Sales E-mail: sales@zyxel.dk
- Telephone: +45-39-55-07-00
- Fax: +45-39-55-07-07
- Web Site: www.zyxel.dk
- Regular Mail: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

Finland

- Support E-mail: support@zyxel.fi
- Sales E-mail: sales@zyxel.fi
- Telephone: +358-9-4780-8411
- Fax: +358-9-4780 8448
- Web Site: www.zyxel.fi
- Regular Mail: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

France

- E-mail: info@zyxel.fr
- Telephone: +33-4-72-52-97-97
- Fax: +33-4-72-52-19-20
- Web Site: www.zyxel.fr
- Regular Mail: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

Germany

- Support E-mail: support@zyxel.de
- Sales E-mail: sales@zyxel.de
- Telephone: +49-2405-690969
- Fax: +49-2405-6909-99
- Web Site: www.zyxel.de
- Regular Mail: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

Hungary

- Support E-mail: support@zyxel.hu
- Sales E-mail: info@zyxel.hu
- Telephone: +36-1-3361649
- Fax: +36-1-3259100
- Web Site: www.zyxel.hu
- Regular Mail: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

Kazakhstan

- Support: <http://zyxel.kz/support>
- Sales E-mail: sales@zyxel.kz

- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web Site: www.zyxel.kz
- Regular Mail: ZyXEL Kazakhstan, 43, Dostyk ave., Office 414, Dostyk Business Centre, 050010, Almaty, Republic of Kazakhstan

North America

- Support E-mail: support@zyxel.com
- Sales E-mail: sales@zyxel.com
- Telephone: +1-800-255-4101, +1-714-632-0882
- Fax: +1-714-632-0858
- Web Site: www.us.zyxel.com
- FTP Site: <ftp.us.zyxel.com>
- Regular Mail: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

Norway

- Support E-mail: support@zyxel.no
- Sales E-mail: sales@zyxel.no
- Telephone: +47-22-80-61-80
- Fax: +47-22-80-61-81
- Web Site: www.zyxel.no
- Regular Mail: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

Poland

- E-mail: info@pl.zyxel.com
- Telephone: +48 (22) 333 8250
- Fax: +48 (22) 333 8251
- Web Site: www.pl.zyxel.com
- Regular Mail: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

Russia

- Support: <http://zyxel.ru/support>
- Sales E-mail: sales@zyxel.ru
- Telephone: +7-095-542-89-29
- Fax: +7-095-542-89-25
- Web Site: www.zyxel.ru
- Regular Mail: ZyXEL Russia, Ostrovityanova 37a Str., Moscow, 117279, Russia

Spain

- Support E-mail: support@zyxel.es
- Sales E-mail: sales@zyxel.es
- Telephone: +34-902-195-420
- Fax: +34-913-005-345

- Web Site: www.zyxel.es
- Regular Mail: ZyXEL Communications, Arte, 21 5ª planta, 28033 Madrid, Spain

Sweden

- Support E-mail: support@zyxel.se
- Sales E-mail: sales@zyxel.se
- Telephone: +46-31-744-7700
- Fax: +46-31-744-7701
- Web Site: www.zyxel.se
- Regular Mail: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

Ukraine

- Support E-mail: support@ua.zyxel.com
- Sales E-mail: sales@ua.zyxel.com
- Telephone: +380-44-247-69-78
- Fax: +380-44-494-49-32
- Web Site: www.ua.zyxel.com
- Regular Mail: ZyXEL Ukraine, 13, Pimonenko Str., Kiev, 04050, Ukraine

United Kingdom

- Support E-mail: support@zyxel.co.uk
- Sales E-mail: sales@zyxel.co.uk
- Telephone: +44-1344 303044, 08707 555779 (UK only)
- Fax: +44-1344 303034
- Web Site: www.zyxel.co.uk
- FTP Site: [ftp.zyxel.co.uk](ftp://ftp.zyxel.co.uk)
- Regular Mail: ZyXEL Communications UK, Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom (UK)

“+” is the (prefix) number you dial to make an international telephone call.

Index

Numerics

802.1P priority [74, 75](#)

A

Access control
 SNMP [180](#)
 access control
 login account [182](#)
 remote management [190](#)
 service [189](#)
 SNMP
 activate IEEE 802.1x [118](#)
 Address Resolution Protocol See ARP
 alarm profile [80, 82](#)
 alternative subnet mask notation [287](#)
 application [31](#)
 curbside [32](#)
 MTU
 ARP [205](#)
 ARP table
 ARP, how it works [205](#)
 automatic VLAN registration
 VLAN
 automatic registration [88](#)

B

backup configuration [174](#)
 bandwidth control [107](#)
 Basic setting [63](#)
 BPDU
 Bridge Protocol Data Unit See BPDU
 broadcast [109](#)
 broadcast storm control [109](#)

C

Canonical Format Indicator See CFI

certifications [295, 296](#)
 notices [296](#)
 viewing [296](#)
 CFI [87](#)
 Change password [50](#)
 CI Commands [213](#)
 Class of Service See CoS
 classifier
 Ethernet type [129](#)
 example [130](#)
 packet format [128](#)
 CLI
 access [210](#)
 access priority [210](#)
 change password [214](#)
 login [212](#)
 login password [214](#)
 logout [217](#)
 management interface [210](#)
 CLI Command
 Configure tagged VLAN example [259](#)
 cluster management [197](#)
 access password [201](#)
 cluster member [201](#)
 cluster member firmware upgrade [199](#)
 clustering candidate [201](#)
 manager [197, 201](#)
 member [197](#)
 member web configurator screen [199](#)
 network example [197](#)
 setup [200](#)
 specification [197](#)
 status [198](#)
 switch models [197](#)
 warning icon [201](#)
 cluster manager [197](#)
 cluster member [197](#)
 clustering [197](#)
 Command
 Forwarding Process Example [263](#)
 Summary [217](#)
 Syntax conventions [212](#)
 command
 exit [217](#)
 command interface [32](#)
 Command Line Interface See CLI
 commands
 modes summary [215](#)
 configuration backup [174](#)

- Configuration file [51](#)
 - Restore [51](#)
- configuration restore [174](#)
- configure port authentication [118](#)
- configuring STP [104](#)
- connection test [191](#)
- Console port
 - Settings [39](#)
- console port [210](#)
 - initial screen [211](#)
- contact information [299](#)
- copyright [295](#)
- CoS [157](#)
- CPU management port [93](#)
- CRC (Cyclic Redundant Check) [61](#)
- create login account [182](#)
- customer support [299](#)

D

- destination lookup failure See DLF
- device MAC address [63](#)
- DHCP [165](#)
 - option 82 [165](#)
 - relay agent information [165](#)
- DHCP relay
- diagnostic [191](#)
 - ping [191](#)
 - system log [191](#)
 - test [191](#)
- Differentiated Services See DiffServ
- Differentiated ServicesSee DS
- DiffServ [133](#), [157](#)
 - activate [158](#)
 - DSCP-to-IEEE802.1p mapping [159](#)
 - marking rule
- DiffServ Code Point See DSCP
- disclaimer [295](#)
- DLF
- double-tagged frame [139](#)
- double-tagged frame format [141](#)
- DS [133](#), [157](#)
- DSCP [157](#)
 - DSCP-to-IEEE802.1p mapping [159](#)
- Dynamic Host Configuration Protocol See DHCP
- dynamic link aggregation

E

- egress port [95](#)
- Ethernet broadcast address [205](#)
- Ethernet port connection [38](#)
- Ethernet port detail [59](#)
- Ethernet ports
 - Default settings [38](#)
- extended authentication protocol [117](#)

F

- fast mode [76](#)
- FCC interference statement [295](#)
- File Transfer Protocol See FTP
- filename convention [175](#)
- Filtering [99](#)
- filtering [99](#)
 - database [203](#)
 - IGMP [145](#)
- Firmware [64](#)
- firmware [173](#)
- firmware upgrade [173](#), [199](#)
- firmware version [63](#)
- fixed rate [76](#)
- Flow control [74](#), [75](#)
 - Back pressure [74](#), [75](#)
 - IEEE802.3x [74](#), [75](#)
- front panel [37](#)
- FTP [33](#), [175](#)
 - command example [175](#)
 - procedure [176](#)
 - restriction [177](#)

G

- GARP
 - Generic Attribute Registration Protocol See GARP
 - join timer [69](#)
 - leave all timer [69](#)
 - leave timer [69](#)
 - timer [69](#), [88](#)
- garp status [260](#)
- GARP timer [88](#)
- general setup [65](#)
- Getting help [52](#)
- Gigabit Ethernet ports [38](#)
- GMT (Greenwich Mean Time) [67](#)

GVRP
 GARP VLAN Registration Protocol See GVRP
 GVRP (GARP VLAN Registration Protocol) [255](#)
 gvrp disable [261](#)
 gvrp enable [261](#)
 gvrp status [261](#)

H

hardware connection [37](#)
 hardware installation [35](#)
 rack mount [35](#)
 hardware monitor [64](#)
 hop count [164](#)
 HTTP [130](#)
 HTTP over SSL See HTTPS
 HTTPS
 example [187](#)
 HyperText Transfer Protocol over Secure Socket Layer See HTTPS

I

IANA [292](#)
 IEEE 802.1p [69](#)
 IEEE 802.1Q [87](#)
 IEEE 802.1w RSTP
 IEEE 802.1x [117](#)
 Note [117](#)
 IEEE 802.3ad
 IGMP [145](#)
 snooping [145](#)
 version
 IGMP filtering [145](#)
 profile [148](#)
 IGMP snooping
 MVR
 In [139](#)
 ingress check [92](#)
 ingress port [95](#)
 interleave delay [76](#)
 Internet Assigned Numbers Authority
 See IANA [292](#)
 Internet Group Multicast Protocol See IGMP
 IP setup [69](#)

L

LACP
 link aggregation ID [114](#)
 note [113](#)
 server [115](#)
 system priority [115](#)
 timeout [116](#)
 latency mode [76](#)
 fast [76](#)
 interleave delay [76](#)
 LED [37](#)
 LEDs [40](#)
 limit MAC address learning [122](#)
 Link Aggregate Control Protocol See LACP
 link aggregation [113](#)
 ID [114](#)
 note [113](#)
 server [116](#)
 timeout [116](#)
 load factory defaults [170](#)
 Lockout [50](#)
 log [191](#)
 logical link [113](#)
 Login [45](#)
 Password [50](#)
 login [212](#)
 Login account
 administrator [182](#)
 login account [182](#)
 account type [182](#)
 non-administrator [183](#)
 number of [182](#)
 login precedence [65](#)
 logout [217](#)

M

MAC address aging time [68](#)
 MAC address filter [99](#)
 MAC address forwarding decision [203](#)
 MAC address learning [68](#), [97](#), [121](#)
 MAC table [203](#)
 disaply [204](#)
 sort [204](#)
 maintenance [169](#)
 backup configuration [174](#)
 firmware upgrade [173](#)
 load factory defaults [170](#)
 restore configuration [174](#)
 managment IP address [70](#)

- management interface
 - CLI [210](#)
- managing the device
 - good habits [33](#)
 - using FTP. See FTP.
 - using SNMP. See SNMP.
 - using Telnet. See command interface.
 - using the command interface. See command interface.
 - using the web configurator. See web configurator.
- MIB
 - supported [181](#)
- MIBs [277](#)
- Mini GBIC ports [38](#)
 - Connection speed [38](#)
 - Connector type [38](#)
 - Transceiver installation [38](#)
 - Transceiver removal [39](#)
- mini-GBIC port connection [38](#)
- monitor port [111](#)
- MSA (MultiSource Agreement) [38](#)
- MTU [31](#)
- MTU (Multi-Tenant Unit) [67](#)
- Multicast [149](#)
- multicast [145](#)
 - address [145](#)
 - setup [146](#)
- multicast group [148](#)
- multicast VLAN [152](#)
- multiple login [210](#)
- Multiple Tenant Unit See also MTU
- MVR
 - configuration [151](#)
 - configuration example [154](#)
 - group configuration [152](#)
 - how it works [150](#)
 - mode [150](#)
 - Multicast VLAN Registration See MVR
 - network example
 - port [150](#)

N

- NAT [292](#)
- Network Element (NE)
- Network Management System (NMS)
- Network Time Protocol See NTP
- NTP [67](#)

O

- Operating Temperature [277](#)
- Operational Humidity [277](#)

P

- Password [50](#)
- Per-Hop Behavior See PHB
- PHB [133](#), [157](#)
- physical queue [69](#)
- ping [191](#)
- policy [133](#)
 - example [137](#)
- POP3 [130](#)
- port
 - and MVR [150](#)
- Port authentication
 - RADIUS server [119](#)
- port authentication [117](#)
- Port Based VLAN Type [68](#)
- port connection [37](#)
- port isolation [92](#), [95](#)
- Port Mirroring [234](#), [255](#)
- Port mirroring [111](#)
- port redundancy [113](#)
- port security [121](#)
 - limit MAC address learning [122](#)
- port setup [72](#)
- Port speed/duplex [74](#)
- port status [53](#)
- port test [191](#)
- Port VID
 - Default for all ports [236](#)
- port VID [87](#)
- port VLAN trunking [89](#)
- port-based VLAN [93](#)
 - port isolation [95](#)
 - setting wizard [95](#)
- POTS port connection [37](#)
- Power Spectral Density See PSD
- priority [69](#)
- priority level [69](#)
- priority queue assignment [69](#)
- product registration [297](#)
- profile
 - alarm [80](#), [82](#)
 - VDSL line [77](#)
- PSD [76](#)

PVID [87](#), [92](#)

Q

QoS [127](#), [157](#)

Quality of Service See QoS

queue weight

Queuing [123](#)

Queuing algorithm [123](#)

queuing algorithm

select [125](#)

SPQ

Queuing method [123](#)

R

rack mouting [35](#)

requirement [35](#)

Radio Frequency Interference See RFI

RADIUS

RADIUS server [117](#)

Advantages [117](#)

Network example [117](#)

Settings [119](#)

setup [119](#)

shared secret [119](#)

UDP port [119](#)

Rapid Spanning Tree Protocol See RSTP

rate adaption [76](#), [79](#)

fixed rate [76](#)

rate adaptive decrease mode [76](#)

rate adaptive decrease mode [76](#)

reauthentication [118](#)

reboot system [170](#)

registration

product [297](#)

related documentation [3](#)

Remote Authentication Dial In User Service See RADIUS

remote management [190](#)

service [189](#), [190](#)

Reset [51](#)

reset configuration [170](#)

reset to the factory defaults [170](#)

restart system [170](#)

Restore configuration [51](#)

restore configuration [174](#)

RFC 2131

RFC 2132

RFC 2138

RFC 2139

RFC 3046 [165](#)

RFC 3164 [193](#)

RFI [77](#)

route cost [164](#)

RSTP

Runt [57](#)

S

Safety [277](#)

safety warnings [6](#)

Secure Shell See SSH

Secure Socket Layer See SSL

select VLAN type [68](#)

service access control [189](#)

service port [190](#)

Service Provider's Network See SPN

SFP (Small Form-factor Pluggable) [38](#)

shared secret [119](#)

Signal-to-Noise Ratio See SNR

Simple Network Management Protocol See SNMP

SNMP [33](#)

agent [180](#)

command [180](#)

community [182](#)

manager [180](#)

network component [180](#)

object variable

Management Information Base See MIB

supported MIB [181](#)

supported version

trap [181](#)

trap destination [182](#)

SNR [76](#)

SP TPID

Service Provider Tag Protocol Identifier See SP TPID

spanning tree

Spanning Tree Protocol (STP) [101](#)

Spanning Tree Protocol See STP

SPN [139](#)

SPQ

SSH [212](#)

how it works [184](#)

implimentation [185](#)

login example [185](#)

requirement [185](#)

standard port [185](#)

- version supported [185](#)
- SSL
- Standards [275](#)
- standby port [113](#)
- static VLAN
 - port setup [92](#)
- static MAC address [97](#), [121](#)
- Static MAC forwarding [97](#)
- static MAC forwarding [97](#)
- static route [163](#)
 - destination IP address [163](#)
 - metric [164](#)
- static VLAN
 - acceptable frame type [93](#)
 - Control [91](#)
 - create [91](#)
 - ingress check [92](#)
 - port isolation [92](#)
 - status [90](#)
 - tagging [91](#)
- Status [46](#)
 - LED [40](#)
 - VLAN [90](#)
- status [53](#)
 - Ethernet port detail [59](#)
 - port [53](#)
 - STP [103](#)
 - VLAN port detail [55](#)
- STP [101](#)
 - Bridge ID [103](#)
 - bridge priority [104](#)
 - designated bridge [102](#)
 - forwarding delay [105](#)
 - Hello BPDU [102](#)
 - hello time [104](#)
 - How it works [102](#)
 - max age [102](#), [105](#)
 - path cost [101](#), [105](#)
 - port priority [105](#)
 - port state [102](#)
 - root path cost [102](#)
 - root port [102](#)
 - setup [104](#)
 - status [103](#)
 - Terminology [101](#)
 - terminology [101](#)
- Strict Priority Queuing See SPQ
- subnet [285](#)
- subnet mask [286](#)
- subnetting [288](#)
- Switch lockout [50](#)
- Switch reset [51](#)
- switch setup [68](#)
- syntax conventions [4](#)
- sys Commands

- examples [243](#), [251](#), [253](#)
- sys log disp [253](#)
- syslog [193](#)
 - log type [194](#)
 - protocol [193](#)
 - server setup [194](#)
 - setup [193](#)
 - severity level [193](#)
- system date [65](#)
- system information [63](#)
- system log [191](#)
- system name [63](#)
- system reboot [170](#)
- system time [65](#)
- System up time [54](#)

T

- Tag Control Information See TCI
- Tag Protocol Identifier See TPID
- TCI
- TCP/UDP protocol port numbers [129](#)
- Telco-50 Connector Pin Assignments [278](#), [281](#)
- Telnet [211](#)
- time format
- time server [67](#)
- time zone [65](#)
- TPID [87](#), [141](#)
- trademarks [295](#)
- Transceiver
 - Installation [38](#)
 - Removal [39](#)
- trap [181](#)
 - destination [182](#)
- trunk group [113](#)
- trunking [113](#)
 - note [113](#)

U

- UPBO [76](#)
- Upstream Power Back Off See UPBO
- USER Telco-50 Connectors [281](#)
- UTC (Universal Time Coordinated) [67](#)

V

VDSL port connection [37](#)
 VDSL port detail [55](#)
 ventilation [35](#)
 VID [90](#), [141](#)
 view log [191](#)
 Virtual Local Area Network See VLAN
 VLA stacking
 frame format [141](#)
 VLAN [67](#), [139](#)
 acceptable frame type [93](#)
 double-tagged frame [139](#)
 IEEE 802.1q parameter
 ingress check [92](#)
 Introduction [67](#)
 number of possible VIDs
 Number of VLANs [90](#)
 port isolation [92](#), [95](#)
 port trunking [89](#)
 port-based [93](#)
 priority frame
 select type [68](#)
 stacking [139](#)
 static
 Status [90](#)
 tag format [141](#)
 tagging [87](#)
 Trunking [89](#)
 Type [89](#)
 VLAN ID [87](#)
 VLAN Identifier See VID
 VLAN profile [77](#)
 VLAN stacking [139](#)
 port role [140](#)
 VLAN tag [87](#)
 VLAN trunking [93](#)
 vlan1q port accept [262](#)
 vlan1q port gvrp [262](#)
 vlan1q svlan active [264](#)
 vlan1q svlan delentry [264](#)
 vlan1q svlan inactive [264](#)
 vlan1q svlan list [264](#)
 vlan1q svlan setentry [262](#)

W

warranty [296](#)
 note [297](#)
 Web configuration
 Screen summary [47](#)

Web configurator
 Getting help [52](#)
 Home [46](#)
 Login [45](#)
 Logout [52](#)
 Navigation panel [46](#)
 web configurator [32](#)
 Weighted Fair Scheduling See WFS
 WFS
 queue weight

Z

ZyNOS (ZyXEL Network Operating System) [175](#)

